



JPP 8/29/02 14:25

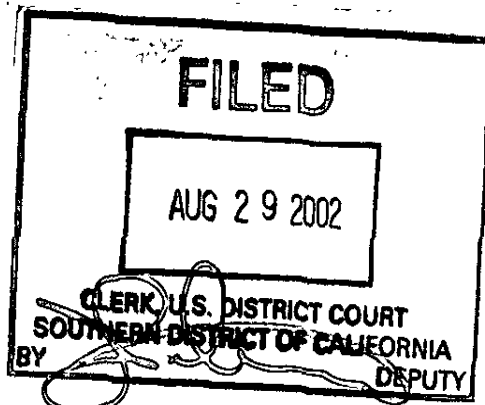
3:02-CV-01727 DIRECTED ELECTRONICS V. DAHLIN

1

CMP.

1 KRISTEN E. CAVERLY (State Bar No. 175070)
2 HENDERSON & CAVERLY LLP
3 P.O. Box 9144 (All U.S. Mail)
4 16236 San Dieguito Road, Suite 1-27
5 Rancho Santa Fe, CA 92067-9144
6 Telephone: (858) 756-6342
7 Facsimile: (858) 756-4732

8 Attorneys for Plaintiff
9 Directed Electronics, Inc.



10 UNITED STATES DISTRICT COURT
11 SOUTHERN DISTRICT OF CALIFORNIA

12 **02 CV 1727 JM (JAH)**
13 Case No.

14 DIRECTED ELECTRONICS, INC., a
15 California corporation

16 Plaintiff,

17 v.

18 STEVE DAHLIN, an individual doing business
19 as THE LONE GUNMEN,

20 Defendant.

21 COMPLAINT FOR:

- 22 1) Federal Patent Infringement (35 U.S.C. § 271);
- 23 2) Federal Trademark Infringement (15 U.S.C. § 1114);
- 24 3) Federal Unfair Competition, False Designation of Origin, and Dilution (15 U.S.C. § 1125(2));
- 25 4) Tortious Interference with Contract;
- 26 5) State Unfair Competition (Cal. Bus. & Prof. Code § 17200);
- 27 6) State False/Misleading Advertisement (Cal. Bus. & Prof. Code § 17500)
- 28 7) State Trademark Infringement (Cal. Bus. & Prof. Code § 14335);
- 8) Dilution and Injury to Business Reputation (Cal Bus. & Prof. Code §§ 14320, 14330); and
- 9) Common Law Unfair Competition

JURY TRIAL DEMANDED

ORIGINAL

GC

1 Plaintiff DIRECTED ELECTRONICS, INC., ("DIRECTED") alleges as follows:

2 **THE PARTIES**

3 1. DIRECTED is a California corporation with its principal place of business at
4 One Viper Way, Vista, California 92083. DIRECTED is engaged in the business of
5 designing, manufacturing and selling, through non-exclusive authorized dealers, vehicle
6 security systems including the VIPER® and PYTHON® vehicle security systems. In June
7 2000, DIRECTED acquired the assets of Clifford Electronics, Inc., including its
8 CLIFFORD® brand of vehicle security systems and the patents and trademarks associated
9 with those products.

10 2. DIRECTED is informed and believes that DEFENDANT Steve Dahlin
11 (hereinafter "DEFENDANT") is an individual doing business as The Lone Gunmen and engaged
12 in the business of selling goods at auction on the Internet, including through websites located at
13 e-bay.com.

14 **JURISDICTION AND VENUE**

15 3. Pursuant to 28 U.S.C. sections 1331 and 1338(a), this Court has original and
16 exclusive jurisdiction in this matter over each of the following claims:

- 17 a. Patent infringement pursuant to 35 U.S.C. section 27;
18 b. Trademark infringement pursuant to 15 U.S.C. sections 1051, *et*.
19 *seq.*; and
20 c. False designation of origin, false description or representation, and
21 dilution in violation of the Lanham Act section 43(a), 15 U.S.C.
22 section 1125(a).

23 4. Pursuant to 28 U.S.C. sections 1331 and 1338(b), this Court has original
24 jurisdiction in this matter over each of the following claims:

- 25 a. Unfair competition; and
26 b. Unfair business practices in violation of California's Business and
27 Professions Code section 17200.

28 ///

1 certificate of registration is attached hereto as Exhibit B and
2 incorporated herein by this reference.

- 3 • VIPER®, United States Trademark Registration No. 1,756,693,
4 issued on March 9, 1993. A true and correct copy of the VIPER®
5 certificate of registration is attached hereto as Exhibit C and
6 incorporated herein by this reference.
- 7 • Forward Facing Snake Image, United States Trademark Registration
8 No. 1,822,608, issued on February 22, 1994 (referred to in
9 advertising as “Vinnie the Viper”). A true and correct copy of the
10 forward facing snake image certificate of registration is attached
11 hereto as Exhibit D and incorporated herein by this reference.
- 12 • DEI®, United States Trademark Registration No. 1,873,747, issued
13 on January 17, 1995. A true and correct copy of the DEI® certificate
14 of registration is attached hereto as Exhibit E and incorporated herein
15 by this reference.
- 16 • Module Case Line Decoration, United States Trademark Registration
17 No. 2,218,082 issued on January 19, 1999 and United States
18 Trademark Registration No. 2,218,081. A true and correct copy of
19 the module case line decoration certificate of registration for No.
20 2,218,082 is attached hereto as Exhibit F and is incorporated herein
21 by this reference.
- 22 • NO ONE DARES COME CLOSE®, United States Trademark
23 Registration No. 1,848,176 issued on August 2, 1994. A true and
24 correct copy of the NO ONE DARES COME CLOSE® certificate of
25 registration is attached hereto as Exhibit G and is incorporated herein
26 by this reference.
- 27 • VIPER With Snake Head and Tail Image, United States Trademark
28 Registration No. 1,961,709 issued on March 12, 1996.

- 1 • WARN AWAY®, United States Trademark Registration No.
2 1,924,872 issued on October 3, 1995.
- 3 • BITWRITER®, United States Trademark Registration No. 2,301,471
4 issued on December 21, 1999.
- 5 • CODE-HOPPING®, United States Trademark Registration No.
6 2,301,162 issued on December 21, 1999.
- 7 • CODE PLUS®, United States Trademark Registration No. 1,943,761
8 issued on December 26, 1995.
- 9 • ESP®, United States Trademark Registration No. 2,315,849 issued
10 on February 8, 2000.
- 11 • FAILSAFE®, United States Trademark Registration No. 1,709,910
12 issued on August 25, 1992.
- 13 • NPC®, United States Trademark Registration No. 2,291,545 issued
14 on November 9, 1999.
- 15 • NUISANCE PREVENTION®, United States Trademark
16 Registration No. 1,937,559 issued on November 21, 1995.
- 17 • REVENGER®, United States Trademark Registration No. 1,962,705
18 issued on March 19, 1996.
- 19 • SOFT CHIRP®, United States Trademark Registration No.
20 1,949,768 issued on January 16, 1996.
- 21 • STINGER®, United States Trademark Registration No. 1,937,900
22 issued on November 28, 1995.
- 23 • VALET®, United States Trademark Registration No. 1,721,572
24 issued on October 6, 1992.
- 25 • VRS®, United States Trademark Registration No. 1,831,266 issued
26 on April 19, 1994.

27 9. DIRECTED is informed and believes that DIRECTED, either itself or its
28 predecessor-in-interest, has continually promoted the sale, through interstate commerce, of its

1 vehicle security products bearing some or all of the above trademarks since the claimed first use
2 of such marks. Among other things, DIRECTED's CLIFFORD®, PYTHON®, VIPER®, NO
3 ONE DARES COME CLOSE®, DEI®, and snake image trademarks are placed on its product
4 packaging, on its product brochures and pamphlets, on banners and window decals, and on
5 miscellaneous promotional merchandise including cups, coffee mugs, posters, t-shirts, etc. Use
6 of the referenced trademarks for these related marketing purposes is covered by separate
7 registrations. DIRECTED also uses its trademarks in television, newspaper and magazine
8 advertisements.

9 10. As a result of DIRECTED's advertising, marketing and other promotional efforts,
10 the CLIFFORD®, PYTHON®, VIPER®, NO ONE DARES COME CLOSE®, DEI®, and
11 snake image trademarks have become widely known and extremely valuable goodwill has
12 developed in each. By virtue of this advertising, marketing and promotion, and the extensive use
13 of these marks, the CLIFFORD®, PYTHON®, VIPER®, NO ONE DARES COME CLOSE®,
14 DEI®, and snake image trademarks also have become distinctive of DIRECTED's goods, and
15 are closely identified with DIRECTED's goodwill and reputation.

16 **Patents**

17 11. Many of the components of DIRECTED's CLIFFORD®, PYTHON® and
18 VIPER® lines of vehicle security systems are covered by utility patents issued by the United
19 States Patent and Trademark Office.

20 12. DIRECTED owns or is a licensee of the following active patents, among others,
21 relating to vehicle security systems:

- 22 • Multi-Featured Security System With Self-Diagnostic Capability,
23 United States Patent No. 4,887,064 issued December 12, 1989. A
24 true and correct copy of Patent No. 4,887,064 is incorporated herein
25 by reference and attached hereto as Exhibit H.
- 26 • Electronic Vehicle Security System, United States Patent No.
27 5,157,375, United States Patent No. 5,157,375 issued October 20,
28

1 1992. A true and correct copy of Patent No. 5,157,375 is
2 incorporated herein by reference and attached hereto as Exhibit I.

3 • Advanced Automotive Automation and Security System, United
4 States Patent No. 5,534,845 issued July 9, 1996. A true and correct
5 copy of Patent No. 5,534,845 is incorporated herein by reference and
6 attached hereto as Exhibit J.

7 • Advanced Method of Indicating Incoming Threat Level to an
8 Electronically Secured Vehicle and Apparatus Therefore, United
9 States Patent No. 5,646,591 issued July 8, 1997. A true and correct
10 copy of Patent No. 5,646,591 is incorporated herein by reference and
11 attached hereto as Exhibit K.

12 • Vehicle Alarm Case Module, United States Patent No. Des. 345,711
13 issued April 5, 1994. A true and correct copy of Patent No. Des.
14 345,711 is incorporated herein by reference and attached hereto as
15 Exhibit L.

16 • Motion Sensitive Security System, United States Patent No.
17 4,584,569 issued April 22, 1986 (Reexamination No. B1 4,584,569
18 issued June 19, 1990). A true and correct copy of Patent
19 No. 4,584,569 is incorporated herein by reference and attached
20 hereto as Exhibit M.

21 • Method of Indicating the Threat Level of an Incoming Shock to an
22 Electronically Secured Vehicle and Apparatus Therefore, United
23 States Patent No. 5,532,670 issued July 2, 1996. A true and correct
24 copy of Patent No. 5,532,670 is incorporated herein by reference and
25 attached hereto as Exhibit N.

26 • Remote Control Transmitter, United States Patent No. Des. 419,474
27 issued January 25, 2000.

28 • Siren, United States Patent No. 345,317 issued March 22, 1994.

- 1 • Car Alarm Having A Soft Chirp Arming Signal, United States Patent
2 No. 5,572,185 issued November 5, 1996.
- 3 • User-Programmable Voice Notification Device for Security Alarm
4 Systems, United States Patent No. 5,245,694 issued September 14,
5 1993.
- 6 • Advanced Embedded Code Hopping System, United States Patent
7 No. 5,872,519 issued February 16, 1999.
- 8 • Alarm Sensor Multiplexing, United States Patent No. 5,783,989
9 issued July 21, 1998.

10 13. DIRECTED's CLIFFORD®, PYTHON® and VIPER® products are covered by
11 one or more claims of the above listed patents.

12 14. DIRECTED is informed and believes that sellers and purchasers of
13 DIRECTED's CLIFFORD®, PYTHON® and VIPER® products have actual or
14 constructive notice of the applicable patents. For example, DIRECTED gives notice to the
15 public of the patents covering its VIPER® vehicle security systems by placing a card or
16 piece of paper in each product box which lists all of DIRECTED's patents by number and
17 states that "This product is covered by one or more of the following U.S. patents...."

18 **Authorized Distribution Only**

19 15. DIRECTED permits its CLIFFORD®, PYTHON® and VIPER® vehicle security
20 systems to be advertised, sold and installed only by its contractually authorized dealers.
21 DIRECTED's dealers are carefully selected, and are, thereafter, trained, supported and
22 monitored by DIRECTED and its representatives. DIRECTED's highly selective dealers are
23 chosen, in part, because they have appropriate facilities and installation equipment and because
24 they have skilled and trained vehicle security system installers.

25 16. DIRECTED has expended, and continues to expend, substantial financial
26 and other resources in an effort to control the quality of the installation of its vehicle
27 security system products. In addition to being highly selective when choosing its dealers,
28 DIRECTED spends significant time, effort and money educating its dealers with respect to

1 DIRECTED's products, and training its dealers with respect to the installation of its vehicle
2 security systems. DIRECTED, at considerable expense, further provides its dealers with
3 "real-time" telephone support and access to computerized information regarding the
4 detailed electrical systems of, and installation and wiring requirements for, numerous
5 domestic and foreign automobiles sold in the United States.

6 17. DIRECTED also visually monitors its authorized dealers from time to time
7 to make sure they are maintaining the necessary quality standards for the sale and
8 installation of DIRECTED's products.

9 18. DIRECTED often terminates authorized dealers if it finds they have violated the
10 terms of their agreement.

11 19. If a CLIFFORD®, PYTHON® or VIPER® vehicle security system is not
12 installed properly, it will not adequately protect against theft of the vehicle. More importantly,
13 faulty installation may interfere with the proper functioning of the vehicle and, as a result, pose a
14 safety risk to the customer and others, including creating a fire hazard. It is for these reasons,
15 among others, that DIRECTED spends considerable time, effort and resources educating,
16 training and supporting its authorized dealers with respect to the sale and installation of its
17 CLIFFORD®, PYTHON® and VIPER® vehicle security systems.

18 20. Maintaining control over the quality of the installation of CLIFFORD®,
19 PYTHON® and VIPER® vehicle security systems is further crucial to DIRECTED because the
20 failure of the system to operate properly -- even though that failure is due to faulty installation as
21 opposed to a defect in the product itself -- will cause the consumer to believe that the product
22 itself is defective. The goodwill and reputation, that DIRECTED has spent substantial time,
23 effort and money developing, will thereby be tarnished and damaged, particularly where the
24 failure of the system to operate properly causes a theft of either the consumer's vehicle or
25 personal property located inside the vehicle. It is for this additional reason, as well as those
26 stated above, that in addition to providing extensive training for its authorized dealers,
27 DIRECTED contractually obligates its authorized dealers to install the vehicle security systems
28 on the dealer's premises, occasionally visits its authorized dealers to observe the quality of

1 installation of its products, makes available to its authorized dealers, by telephone, the technical
2 representatives capable of assisting the dealers with installation problems as they arise, and
3 provides the computer software to its authorized dealers containing the electronic circuitry for
4 numerous domestic and foreign vehicles sold in the United States and abroad.

5 21. To further maintain control over the quality of its product installation,
6 DIRECTED does not permit its authorized dealers to sell DIRECTED's CLIFFORD®,
7 PYTHON® or VIPER® vehicle security systems to anyone who is not an ultimate consumer,
8 and they are not permitted to sell CLIFFORD®, PYTHON® or VIPER® vehicle security
9 systems to an ultimate consumer unless the alarm is installed by the authorized dealer on the
10 authorized dealer's premises.

11 22. At the time of the actions complained of herein, DEFENDANT was not an
12 authorized dealer of CLIFFORD®, PYTHON® or VIPER® products.

13 **Warranty**

14 23. As one of its primary marketing tools, DIRECTED includes with each
15 CLIFFORD®, PYTHON® and VIPER® vehicle security system its limited lifetime consumer
16 warranty. DIRECTED has expended substantial time and money in making the general public
17 aware of the benefits of the warranty.

18 24. DIRECTED will not honor its limited lifetime warranty on products purchased
19 from unauthorized dealers.

20 25. It is specifically stated in the warranty that it is valid if "the unit was
21 professionally installed and serviced by an authorized Directed dealer." Thus, anyone
22 purchasing a CLIFFORD®, PYTHON®, or VIPER® vehicle security system from an
23 unauthorized dealer or an authorized dealer who sold the product without installation does not
24 receive any warranty or guarantee of the product from DIRECTED. A true and correct copy of
25 the terms of DIRECTED's limited lifetime warranty is attached hereto as Exhibit O and
26 incorporated herein by this reference.

27 26. DIRECTED's ongoing business depends heavily upon the proper functioning of
28 its CLIFFORD®, PYTHON® and VIPER® vehicle security systems in vehicles in which it is

1 installed, on the valuable reputation it has developed as a result of the quality of its product and
2 its installation, and on the goodwill it has developed through the sale, promotion and marketing
3 of its products and its DEI®, CLIFFORD®, PYTHON®, VIPER® and snake image and other
4 trademarks. The warranty has further contributed to the excellent reputation DIRECTED enjoys
5 with the general public with respect to its products.

6 **Defendant's Conduct**

7 27. DIRECTED is informed and believes that, subsequent to the adoption and use by
8 DIRECTED of its CLIFFORD®, PYTHON® and VIPER® trademarks for vehicle security
9 systems, DEFENDANT, who is not a DIRECTED authorized dealer, commenced advertising
10 and marketing vehicle security systems by using the trademarks to draw in customers.

11 DIRECTED is informed and believes that DEFENDANT is continuing to advertise using
12 DIRECTED's registered trademarks.

13 28. DIRECTED is informed and believes that DEFENDANT has falsely represented
14 to the public through advertising with the CLIFFORD®, PYTHON® and VIPER® marks that
15 DEFENDANT is authorized by DIRECTED to sell and/or advertise CLIFFORD®, PYTHON®
16 and VIPER® products.

17 29. DIRECTED is informed and believes that, despite not being an authorized dealer,
18 DEFENDANT has sold and offered for sale CLIFFORD®, PYTHON® and VIPER® vehicle
19 security systems to end user customers and/or to distributors.

20 30. DEFENDANT has sold CLIFFORD®, PYTHON® and VIPER® vehicle security
21 systems uninstalled and, thus, without any knowledge, concern or control as to whether the
22 vehicle security system is ever installed, and, if so, whether the system is installed correctly.

23 31. DEFENDANT claims in the description of its products that the products "come
24 complete with all the parts and paperwork." DIRECTED will not honor any warranty for these
25 products.

26 32. DIRECTED is informed and believes that DEFENDANT knows or by the
27 exercise of reasonable care should know that DIRECTED sells its CLIFFORD®, PYTHON®
28 and VIPER® vehicle security systems through authorized dealers only and they are permitted to

1 resell only with installation. This fact is generally known in the car alarm resale industry. And,
2 DIRECTED expressly informed DEFENDANT that DIRECTED's CLIFFORD®, PYTHON®
3 and VIPER® vehicle security systems are sold only through authorized dealers and only to end
4 users in an installed condition. DIRECTED has demanded that DEFENDANT stop selling
5 DIRECTED's CLIFFORD®, PYTHON® and VIPER® vehicle security systems and using its
6 registered trademarks to promote the sale of products. DIRECTED is informed and believes that
7 DEFENDANT has refused to stop his improper activities and continues to use DIRECTED's
8 registered trademarks and sell its products without DIRECTED's authority or consent.

9 33. The unauthorized promotion and sale of DIRECTED's CLIFFORD®,
10 PYTHON® and VIPER® vehicle security systems by DEFENDANT, his failure to maintain
11 control over the quality of the installation of the system, and his use of DIRECTED's registered
12 trademarks and patented materials without DIRECTED's authorization or consent, have caused
13 damage to DIRECTED's reputation and goodwill and to the value of DIRECTED's
14 CLIFFORD®, PYTHON®, VIPER®, DEI® and other trademarks and its patents.

15 **First Cause of Action**

16 **Federal Patent Infringement**

17 **35 U.S.C. Section 271**

18 34. DIRECTED refers to and incorporates herein by reference paragraphs 1
19 through 33 of this Complaint as though set forth in full herein.

20 35. DIRECTED sells its CLIFFORD®, PYTHON® and VIPER® vehicle
21 security systems only through authorized dealers who have entered into a written agreement
22 with DIRECTED which expressly prohibits the authorized dealer from reselling
23 CLIFFORD®, PYTHON® and VIPER® products to anyone other than the end user in an
24 installed condition. DIRECTED is informed and believes that the terms and conditions of
25 DIRECTED's authorized dealer agreements, including the resale restrictions, are known in
26 the car alarm retail industry and are or should in the exercise of reasonable care be known
27 to DEFENDANT. True and correct copies of DIRECTED's form authorized dealer

28 ///

1 agreement, as it currently exists is incorporated herein by reference and attached hereto as
2 Exhibit P.

3 36. DEFENDANT has infringed and is believed to be directly infringing,
4 literally or under the doctrine of equivalents, Patent Nos. 4,887,064 (multi-featured security
5 system with self-diagnostic capability); 5,157,375 (electronic vehicle security system);
6 5,534,845 (advanced automotive and security system); 4,584,569 (motion sensitive security
7 system); Des. 345,711 (vehicle alarm case module); 5,532,670 (method of indicating
8 threat); and 5,646,591 (advanced method of indicating threat), within the United States in
9 violation of 35 U.S.C. section 271(a) by selling and/or offering for sale within this judicial
10 district, without license from DIRECTED, products which incorporate and utilize the
11 inventions and/or designs claimed in the patents listed previously in this paragraph.

12 37. DIRECTED is informed and believes that DEFENDANT has contributed to
13 and are contributing to the infringement of Patent Nos. 4,887,064 (multi-featured security
14 system with self-diagnostic capability); 5,157,375 (electronic vehicle security system);
15 5,534,845 (advanced automotive and security system); 4,584,569 (motion sensitive security
16 system); Des. 345,711 (vehicle alarm case module); 5,532,670 (method of indicating
17 threat); and 5,646,591 (advanced method of indicating threat) in violation of 35 U.S.C.
18 section 271(c). DIRECTED is informed and believes that DEFENDANT has induced and
19 is continuing to induce one or more of DIRECTED's authorized dealers and/or end users to
20 infringe the patents listed previously in this paragraph in violation of 35 U.S.C. § 271(b).

21 38. DIRECTED has no adequate remedy at law and is, therefore, entitled to a
22 preliminary and permanent injunction prohibiting further infringement by DEFENDANT.

23 39. DEFENDANT's infringing activities have been and are willful and
24 deliberate. DIRECTED is entitled to recover treble damages pursuant to 35 U.S.C. section
25 284, reasonable attorneys' fees and expenses of litigation pursuant to 35 U.S.C. section 285,
26 and prejudgment interest pursuant to 35 U.S.C. section 284.

27 40. As a result of DEFENDANT's infringing activities, DIRECTED has been
28 damaged in an amount to be proved at trial, but believed to be in excess of \$100,000. At a

1 minimum, DIRECTED is entitled to recover a reasonable royalty for the acts of
2 infringement by DEFENDANT.

3 **Second Cause of Action**

4 **Federal Trademark Infringement**

5 **15 U.S.C. Section 1114**

6 41. DIRECTED refers to and incorporates herein by reference paragraphs 1
7 through 40 of this Complaint as though set forth in full herein.

8 42. DEFENDANT has been using, in interstate commerce, DIRECTED's
9 registered trademarks, including CLIFFORD®, PYTHON®, VIPER®, DEI®, NO ONE
10 DARES COME CLOSE®, module case design and/or the snake image, without
11 DIRECTED's consent, in connection with the sale, offering for sale, distribution and/or
12 advertising of vehicle security systems, including the unauthorized sale and offering for
13 sale of vehicle security systems manufactured by DIRECTED.

14 43. The use of DIRECTED's trademarks in connection with the promotion, sale,
15 offering for sale and advertising of vehicle security systems by DEFENDANT likely causes
16 confusion, mistake and/or deception, and has caused confusion, mistake and/or deception,
17 in that such use is likely to, and does, deceive the public into believing that there is an
18 association between DIRECTED and DEFENDANT, that the CLIFFORD®, PYTHON® or
19 VIPER® product the consumer purchases is a complete product with all of its component
20 parts and literature, that the control DIRECTED exercises over the quality of the
21 installation of the CLIFFORD®, PYTHON® or VIPER® vehicle security system is being
22 exercised in connection with the purchase and installation of such a security system from
23 DEFENDANT, and that DIRECTED's standard warranties and guarantees apply, when in
24 fact there is no such association, there is no quality control of the product by
25 DEFENDANT, there is no such exercise of control by DIRECTED over the installation of
26 the vehicle security system, and DIRECTED's limited lifetime warranty does not apply.

27 44. To further the confusion, mistake and/or deception caused by
28 DEFENDANT's unauthorized use of DIRECTED's registered trademarks, DIRECTED is

1 informed and believes that DEFENDANT informs customers that he is a DIRECTED
2 authorized dealer and/or when selling CLIFFORD®, PYTHON® and VIPER® products
3 includes therewith DIRECTED's standard limited lifetime warranty. In fact, the limited
4 lifetime warranty is not applicable because the product is not being sold and/or installed by
5 a DIRECTED authorized dealer.

6 45. DEFENDANT's unauthorized use of DIRECTED's trademarks, and the
7 unauthorized advertising and sale of DIRECTED's CLIFFORD®, PYTHON® and
8 VIPER® vehicle security systems constitutes unlawful infringement of DIRECTED's
9 CLIFFORD®, PYTHON® and VIPER®, snake image and other trademarks under the
10 Lanham Act, 15 U.S.C. section 1114.

11 46. DEFENDANT's acts herein alleged were willful, entitling DIRECTED to
12 recover DEFENDANT's profits, damages sustained by DIRECTED, treble damages and
13 costs.

14 47. As a result of DEFENDANT's improper and unauthorized activities,
15 DIRECTED has suffered, and will continue to suffer damages in an amount to be proved at
16 trial, but believed to be in excess of \$100,000.

17 48. DIRECTED has incurred and will continue to incur attorneys' fees in the
18 prosecution of this action and is entitled to recover such fees pursuant to 15 U.S.C. section
19 1117(a).

20 49. Unless and until this Court restrains and enjoins DEFENDANT from using
21 DIRECTED's trademarks and from selling, offering for sale and advertising DIRECTED's
22 CLIFFORD®, PYTHON® and VIPER® vehicle security systems, DEFENDANT will
23 continue his unauthorized and improper activities.

24 ///

25 ///

26 ///

27

28

1 **Third Cause of Action**

2 **Federal Unfair Competition/False Designation of Origin**

3 **15 U.S.C. Section 1125(a)**

4 50. DIRECTED refers to and incorporates herein by reference paragraphs 1
5 through 49 of this Complaint as though set forth in full herein.

6 51. DEFENDANT's unauthorized use of DIRECTED's trademarks and patented
7 technology, and DEFENDANT's express or implied misrepresentations concerning his
8 affiliation with DIRECTED and/or the applicability of DIRECTED's limited lifetime
9 warranty in connection with the promotion, offering for sale and sale of vehicle security
10 systems, constitutes a false designation of origin and/or false and misleading
11 representations, works and symbols in violation of section 43(a) of the Lanham Act, 15
12 U.S.C. section 1125(a).

13 52. As a result of DEFENDANT's improper and unauthorized activities,
14 DIRECTED has suffered and will suffer damages in an amount to be proved at trial, but
15 believed to be in excess of \$100,000.

16 53. DIRECTED has incurred and will continue to incur attorneys' fees and costs
17 in the prosecution of this lawsuit.

18 **Fourth Cause of Action**

19 **Tortious Interference with Contract**

20 54. DIRECTED refers to and incorporates herein by reference paragraphs 1
21 through 53 of this Complaint as though set forth in full herein.

22 55. DIRECTED is informed and believes that DEFENDANT knows, or by the
23 exercise of reasonable care should know, that DIRECTED sells CLIFFORD®, PYTHON®
24 and VIPER® products only to authorized dealers who are contractually obligated to resell
25 the products in an installed condition, to ultimate consumers, and over whom DIRECTED
26 can exercise control with respect to the content and installation of its CLIFFORD®,
27 PYTHON® and VIPER® vehicle security systems.

28 ///

1 California's Unfair Trade Practices Act, California Business & Professions Code sections
2 17200 *et. seq.*

3 61. DEFENDANT's unfair and deceptive business practices have damaged
4 DIRECTED in an amount to be proved at trial, but believed to be in excess of \$100,000.

5 62. DEFENDANT's unfair and deceptive business practices have and will
6 continue to injure DIRECTED, its authorized dealers and the public unless and until they
7 are enjoined by this Court.

8 **Sixth Cause of Action**

9 **State False/Misleading Advertisement**

10 **Cal. Bus. & Prof. Code Section 17500**

11 63. DIRECTED refers to and incorporates herein by reference paragraphs 1
12 through 62 of this Complaint as though set forth in full herein.

13 64. DEFENDANT's use of DIRECTED's trademarks and patented material to
14 sell CLIFFORD®, PYTHON® and VIPER® products and/or entice the public into
15 DEFENDANT's establishment for the purpose of selling DIRECTED's competitors'
16 products and DEFENDANT's false and/or misleading representations, express or implied,
17 that DIRECTED's limited warranty applies to sales made by DEFENDANT constitutes
18 false and/or misleading advertisement in violation of California Business and Professions
19 Code sections 17500 *et seq.*

20 65. DEFENDANT's unfair and deceptive business practices have damaged
21 DIRECTED in an amount to be proved at trial, but believed to be in excess of \$100,000.

22 66. DEFENDANT's unfair and deceptive business practices have and will
23 continue to injure DIRECTED, its authorized dealers and the public unless and until they
24 are enjoined by this Court.

25 ///

26 ///

27 ///

28

PRAYER

WHEREFORE, DIRECTED prays for relief as follows:

As to the first, second, third, fifth, sixth, seventh, and eighth causes of action:

79. For an injunction enjoining DEFENDANT, his agents, affiliates, employees, and those persons in active concert or participation or privity with them who receive actual notice of the order by personal service or otherwise, from infringing DIRECTED's patents, including but not limited to the following: Patent Nos. 4,887,064 (multi-featured security system with self-diagnostic capability); 5,157,375 (electronic vehicle security system); 5,534,845 (advanced automotive and security system); 4,584,569 (motion sensitive security system); Des. 345,711 (vehicle alarm case module); 5,532,670 (method of indicating threat); and 5,646,591 (advanced method of indicating threat);

80. For an injunction enjoining DEFENDANT, his agents, affiliates, employees, and those persons in active concert or participation or privity with them who receive actual notice of the order by personal service or otherwise, from selling or advertising DIRECTED's vehicle security systems without authorization, or using DIRECTED's CLIFFORD®, PYTHON® and VIPER® or other trademarks;

81. For an order requiring DEFENDANT to immediately cease all advertising containing DIRECTED's CLIFFORD®, PYTHON® and VIPER® trademarks and immediately deliver such items to DIRECTED;

82. For an order requiring DEFENDANT to deliver to DIRECTED all CLIFFORD®, PYTHON® and VIPER® vehicle security systems within his possession;

83. For an order precluding DEFENDANT from using any false designation of origin or false description, including DIRECTED's CLIFFORD®, PYTHON® and VIPER® trademarks, that can, or is likely, to lead the consuming public, or individual members thereof, to believe that any product manufactured, distributed or sold by DEFENDANT is in any manner associated or connected with DIRECTED, or is sold, licensed, warranted, sponsored, approved or authorized by DIRECTED;

///

1 84. For a judgment and order that DEFENDANT be required to supply DIRECTED
2 with a complete record of all transactions, agreement, and other activities involving or connected
3 with the purchase, making, using, or selling of infringing devices or activities;

4 85. For an order directing DEFENDANT to file with the Court and serve upon
5 DIRECTED's counsel within thirty days after entry of the order of injunction, a report setting
6 forth the manner and form in which the DEFENDANT has complied with the above specified
7 terms of injunction; and

8 86. For an order awarding to DIRECTED all of DEFENDANT's profits or gains of
9 any kind resulting from DEFENDANT's unauthorized sale and/or advertising of DIRECTED's
10 products, and/or DIRECTED's lost profits and other damages as may be proven, and/or a
11 reasonable royalty for DEFENDANT's unauthorized sales and/or advertising of DIRECTED's
12 products.

13 **As to all causes of action:**

14 87. For monetary damages in an amount according to proof; and

15 88. For interest on said damages at the legal rate from and after the date such
16 damages were incurred.

17 **As to the first, second, fourth, and ninth causes of action:**

18 89. For punitive and exemplary damages.

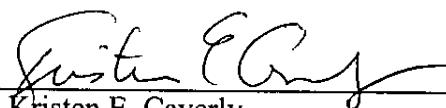
19 **As to all causes of action:**

20 90. For costs, including reasonable attorneys fees; and

21 91. For such other and further relief as the Court deems proper.

23 DATED: August 29, 2002

HENDERSON & CAVERLY LLP

25 By 
26 Kristen E. Caverly
27 Attorneys for Plaintiff Directed
28 Electronics, Inc.

DEMAND FOR JURY TRIAL

Plaintiff DIRECTED hereby demands trial by jury.

DATED: August 29, 2002

HENDERSON & CAVERLY LLP

By 

Kristen E. Caverly
Attorneys for Plaintiff Directed
Electronics, Inc.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF EXHIBITS

<u>Exhibit Tab</u>	<u>Description</u>	<u>Page No.</u>
A	Certificate of Registration for CLIFFORD®, United States Trademark Registration No. 1,674,046, issued on February 4, 1992	24
B	Certificate of Registration for PYTHON®, United States Trademark Registration No. 1,822,606, issued on February 22, 1994	26
C	Certificate of Registration for VIPER®, United States Trademark Registration No. 1,756,693, issued on March 9, 1993	27
D	Certificate of Registration for Forward Facing Snake Image, United States Trademark Registration No. 1,822,608, issued on February 22, 1994	28
E	Certificate of Registration for DEI®, United States Trademark Registration No. 1,873,747, issued on January 17, 1995	29
F	Certificate of Registration for Module Case Line Decoration, United States Trademark Registration No. 2,218,082 issued on January 19, 1999	30
G	Certificate of Registration for NO ONE DARES COME CLOSE®, United States Trademark Registration No. 1,848,176 issued on August 2, 1994	31
H	Multi-Featured Security System With Self-Diagnostic Capability, United States Patent No. 4,887,064 issued December 12, 1989	32
I	Electronic Vehicle Security System, United States Patent No. 5,157,375, United States Patent No. 5,157,375 issued October 20, 1992	99
J	Advanced Automotive Automation and Security System, United States Patent No. 5,534,845 issued July 9, 1996	162
K	Advanced Method of Indicating Incoming Threat Level to an Electronically Secured Vehicle and Apparatus Therefore, United States Patent No. 5,646,591 issued July 8, 1997	205
L	Vehicle Alarm Case Module, United States Patent No. Des. 345,711 issued April 5, 1994	236
M	Motion Sensitive Security System, United States Patent No. 4,584,569 issued April 22, 1986 (Reexamination No. B1 4,584,569 issued June 19, 1990)	238
N	Method of Indicating the Threat Level of an Incoming Shock to an Electronically Secured Vehicle and Apparatus Therefore, United States Patent No. 5,532,670 issued July 2, 1996	254
O	Directed's limited lifetime warranty	268
P	Directed's form authorized dealer agreement, as it exists and as it existed with Directed's predecessor-in-interest Clifford Electronics, Inc.	270

The United States of America



Nº 1674046

CERTIFICATE OF REGISTRATION

This is to certify that the records of the Patent and Trademark Office show that an application was filed in said Office for registration of the Mark shown herein, a copy of said Mark and pertinent data from the Application being annexed hereto and made a part hereof,

And there having been due compliance with the requirements of the law and with the regulations prescribed by the Commissioner of Patents and Trademarks,

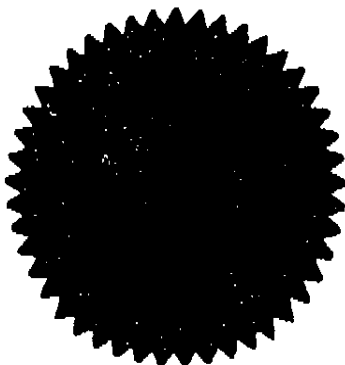
Upon examination, it appeared that the applicant was entitled to have said Mark registered under the Trademark Act of 1946, as amended, and the said Mark has been duly registered this day in the Patent and Trademark Office on the

PRINCIPAL REGISTER

to the registrant named herein.

This registration shall remain in force for TEN years unless sooner terminated as provided by law.

In Testimony Whereof I have hereunto set my hand and caused the seal of the Patent and Trademark Office to be affixed this fourth day of February 1992.



Harry F. Manbeck, Jr.

Commissioner of Patents and Trademarks

Int. Cls.: 9 and 12

Prior U.S. Cls.: 21 and 26

United States Patent and Trademark Office

Reg. No. 1,674,046

Registered Feb. 4, 1992

**TRADEMARK
PRINCIPAL REGISTER**

CLIFFORD

CLIFFORD ELECTRONICS, INC. (CALIFORNIA CORPORATION)
20750 LASSEN STREET
CHATSWORTH, CA 91311

FOR: SECURITY SYSTEMS FOR HOMES COMPRISING CONTROL MODULES, SENSORS, DOOR AND WINDOW TRIGGERS, SIRENS; REMOTELY CONTROLLED STARTER EQUIPMENT FOR REMOTELY STARTING THE ENGINES OF VEHICLES SUCH AS AUTOMOBILES; CONVENIENCE ELECTRONIC ACCESSORIES FOR VEHICLES; NAMELY, ELECTRONIC MODULES FOR DOORS, SEATS, WINDOWS, AND ENGINE CONTROL; REMOTE CONTROL RECEIVERS AND

TRANSMITTERS FOR HOME CONVENIENCE USE, IN CLASS 9 (U.S. CLS. 21 AND 26).

FIRST USE 1-11-1988; IN COMMERCE 1-11-1988.

FOR: SECURITY SYSTEMS FOR AUTOMOBILES, BOATS AND AIRPLANES COMPRISING CONTROL MODULES, DOOR, WINDOW, HOOD AND TRUNK TRIGGERS, SENSORS, SIRENS, IN CLASS 12 (U.S. CLS. 21 AND 26).

FIRST USE 8-0-1976; IN COMMERCE 6-0-1979.

SER. NO. 74-082,626, FILED 7-27-1990.

R. M. FEELEY, EXAMINING ATTORNEY.

Int. Cl.: 12

Prior U.S. Cls.: 19 and 21

United States Patent and Trademark Office

Reg. No. 1,822,606
Registered Feb. 22, 1994

**TRADEMARK
PRINCIPAL REGISTER**

PYTHON

DIRECTED ELECTRONICS, INC. (CALIFORNIA CORPORATION)
2560 PROGRESS STREET
VISTA, CA 92083

FOR: AUTOMOTIVE ANTI-THEFT SYSTEMS COMPRISING ELECTRONIC SENSORS, ELECTRONIC PAIN GENERATORS, ELECTRONIC SIRENS AND REMOTE CONTROL TRANSMITTERS AND RECEIVERS SOLD AS A UNIT THROUGH MAIL ORDER AND THROUGH

RETAIL STORES AND AUTOMOTIVE SECURITY INSTALLERS, IN CLASS 12 (U.S. CLS. 19 AND 21).

FIRST USE 4-16-1986; IN COMMERCE 4-16-1986.

SER. NO. 74-364,190, FILED 3-2-1993.

RICHARD A. STRASER, EXAMINING ATTORNEY

Int. Cl.: 12

Prior U.S. Cls.: 19 and 21

United States Patent and Trademark Office Reg. No. 1,756,693
Registered Mar. 9, 1993

TRADEMARK
PRINCIPAL REGISTER

VIPER

DIRECTED ELECTRONICS, INC. (CALIFORNIA CORPORATION)
1413 LINDA VISTA DRIVE
SAN MARCOS, CA 92069

FOR: VEHICULAR ANTI-THEFT AND SECURITY SYSTEMS; NAMELY, REMOTELY ACTUATED, ELECTRONICALLY-ENERGIZED SECURITY HARDWARE COMPRISING DOOR

LOCKS, ACTUATORS, AUDIBLE ALARMS AND PARTS THEREFOR, IN CLASS 12 (U.S. CLS. 19 AND 21).

FIRST USE 11-9-1984; IN COMMERCE 11-9-1984.

SER. NO. 73-775,611, FILED 1-23-1989.

G. T. GLYNN, EXAMINING ATTORNEY

Int. Cl.: 12

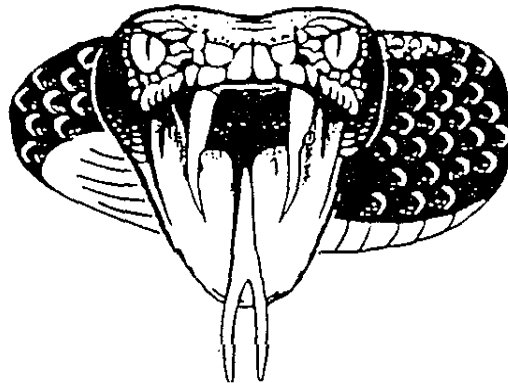
Prior U.S. Cls.: 19 and 21

United States Patent and Trademark Office

Reg. No. 1,822,608

Registered Feb. 22, 1994

**TRADEMARK
PRINCIPAL REGISTER**



DIRECTED ELECTRONICS, INC. (CALIFORNIA CORPORATION)
2560 PROGRESS STREET
VISTA, CA 92083

FOR: AUTOMOTIVE ANTI-THEFT SYSTEMS COMPRISING ELECTRONIC SENSORS, ELECTRONIC PAIN GENERATORS, ELECTRONIC SIRENS, REMOTE CONTROL TRANSMITTERS, REMOTE CONTROL RECEIVERS, SOLD AS A UNIT, AND SOLD THROUGH MAIL ORDER.

RETAIL STORES AND BY AUTOMOTIVE SECURITY INSTALLERS, IN CLASS 12 (U.S. CLS. 19 AND 21).

FIRST USE 6-8-1988; IN COMMERCE 6-8-1988.

SER. NO. 74-385,813. FILED 5-3-1993.

RICHARD A. STRASER, EXAMINING ATTORNEY

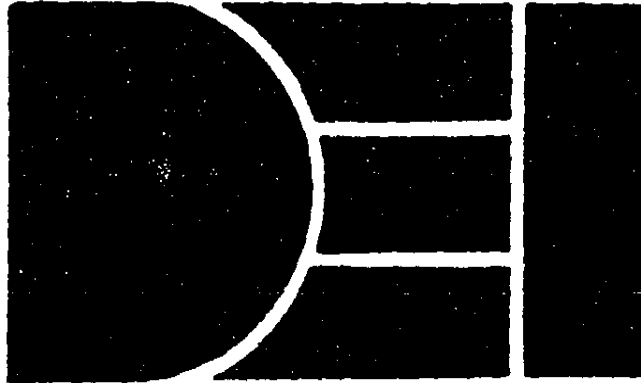
Int. Cl.: 12



Prior U.S. Cls.: 19 and 21

United States Patent and Trademark Office Reg. No. 1,873,747
Registered Jan. 17, 1995

**TRADEMARK
PRINCIPAL REGISTER**



DIRECTED ELECTRONICS, INC. (CALIFOR-
NIA CORPORATION)
2560 PROGRESS STREET
VISTA, CA 92083

FIRST USE 6-0-1989; IN COMMERCE
6-0-1989.

SER. NO. 74-348,752, FILED 1-15-1993.

FOR: ANTI-THEFT ALARMS FOR VEHI-
CLES, IN CLASS 12 (U.S. CLS. 19 AND 21).

ANTHONY R. MASIELLO, EXAMINING AT-
TORNEY

Int. Cl.: 12

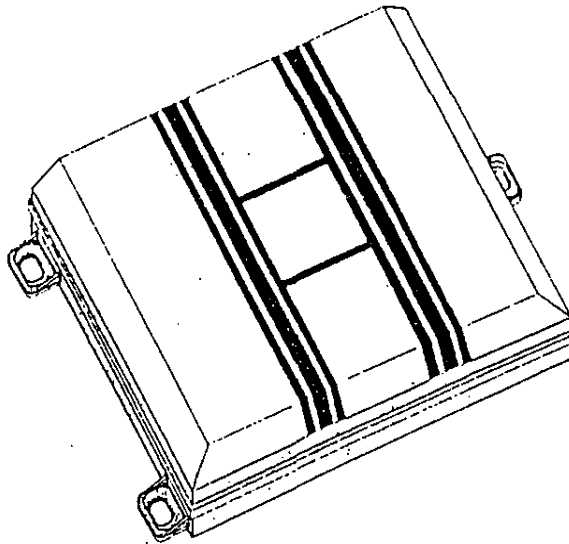
Prior U.S. Cls.: 19, 21, 23, 31, 35 and 44

Reg. No. 2,218,082

United States Patent and Trademark Office

Registered Jan. 19, 1999

TRADEMARK
PRINCIPAL REGISTER



DIRECTED ELECTRONICS, INC. (CALIFORNIA CORPORATION)
2560 PROGRESS STREET
VISTA, CA 92083

FOR: ANTI-THEFT ALARMS FOR VEHICLES; ANTI-THEFT ALARM SYSTEMS COMPRISING ELECTRONIC SENSORS, SIRENS, REMOTE CONTROL TRANSMITTERS, RECEIVERS AND PARTS FOR THE SAME, SOLD SEPARATELY OR AS A UNIT, IN CLASS 12 (U.S. CLS. 19, 21, 23, 31, 35 AND 44).

FIRST USE 1-1-1994; IN COMMERCE 1-1-1994.

GEOMETRIC ARRANGEMENT OF A PARALLEL PAIR OF TRIPLE PARALLEL LINES JOINED BY A PAIR OF PERPENDICULAR LINES.

SER. NO. 75-185,035, FILED 10-17-1996.

MATTHEW KLINE, EXAMINING ATTORNEY



Int. Cl.: 12

Prior U.S. Cls.: 19 and 21

United States Patent and Trademark Office **Reg. No. 1,848,176**
Registered Aug. 2, 1994

**TRADEMARK
PRINCIPAL REGISTER**

NO ONE DARES COME CLOSE

DIRECTED ELECTRONICS, INC. (CALIFORNIA CORPORATION)
2560 PROGRESS STREET
VISTA, CA 92083

FOR: ANTI-THEFT AUTOMOTIVE DEVICES; NAMELY, AUTOMOTIVE ANTI-THEFT ALARMS, ELECTRONIC SENSORS, ELECTRONIC SIRENS, REMOTE CONTROL TRANSMITTERS AND RECEIVERS AND PARTS FOR THE ALARM AND SIREN ONLY SOLD AS A

UNIT AND SOLD THROUGH AUTOMOTIVE SECURITY INSTALLERS, IN CLASS 12 (U.S. CLS. 19 AND 21).

FIRST USE 1-24-1986; IN COMMERCE 1-24-1986.

SN 74-337,339, FILED 12-7-1992.

RICHARD A. STRASER, EXAMINING ATTORNEY

United States Patent [19]

[11] **Patent Number:** 4,887,064

Drori et al.

[45] **Date of Patent:** Dec. 12, 1989

- [54] **MULTI-FEATURED SECURITY SYSTEM WITH SELF-DIAGNOSTIC CAPABILITY**
- [75] **Inventors:** Ze'ev Drori, Chatsworth; Mansoor M. Amirpoor, Northridge, both of Calif.
- [73] **Assignee:** Clifford Electronics, Inc., Chatsworth, Calif.
- [21] **Appl. No.:** 138,828
- [22] **Filed:** Dec. 28, 1987
- [51] **Int. Cl.⁴** B60R 25/00
- [52] **U.S. Cl.** 340/426; 340/528; 340/825.31
- [58] **Field of Search** 340/63, 64, 825.31, 340/825.32, 825.69, 513, 825.49, 524, 528, 654, 426, 430; 307/10 AT, 10.2

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,588,891	6/1971	Porter, Jr.	340/513
3,691,396	9/1972	Hinrichs	340/64 X
3,794,967	2/1974	Fischer	340/63
3,815,088	6/1974	Kumpfbek et al.	340/63
3,858,175	12/1974	Kopera, Jr.	340/63
3,883,895	5/1975	Fecteau	340/224
4,141,009	2/1979	Fowler	340/63 X
4,159,466	6/1979	Mengel	340/63
4,162,479	7/1979	Nickell et al.	340/63
4,174,516	11/1979	Cleary	340/63
4,314,232	2/1982	Tsunoda	340/52 F
4,383,242	5/1983	Sassover et al.	340/64
4,506,253	3/1985	Mande et al.	340/513 X
4,591,834	5/1986	Kyle	340/825.49 X
4,663,626	5/1987	Smith	340/825.69
4,754,255	6/1988	Sanders et al.	340/64
4,794,368	12/1988	Grossheim et al.	340/63

OTHER PUBLICATIONS

"Car Intruder Alarm", *Practical Electronics*, vol. 15, No. 4, p. 22, Apr. 1979.

"Car Theft Alarm", *Practical Electronics*, vol. 17, No. 7, p. 9, Jul. 1981.

Primary Examiner—Joseph A. Orsino

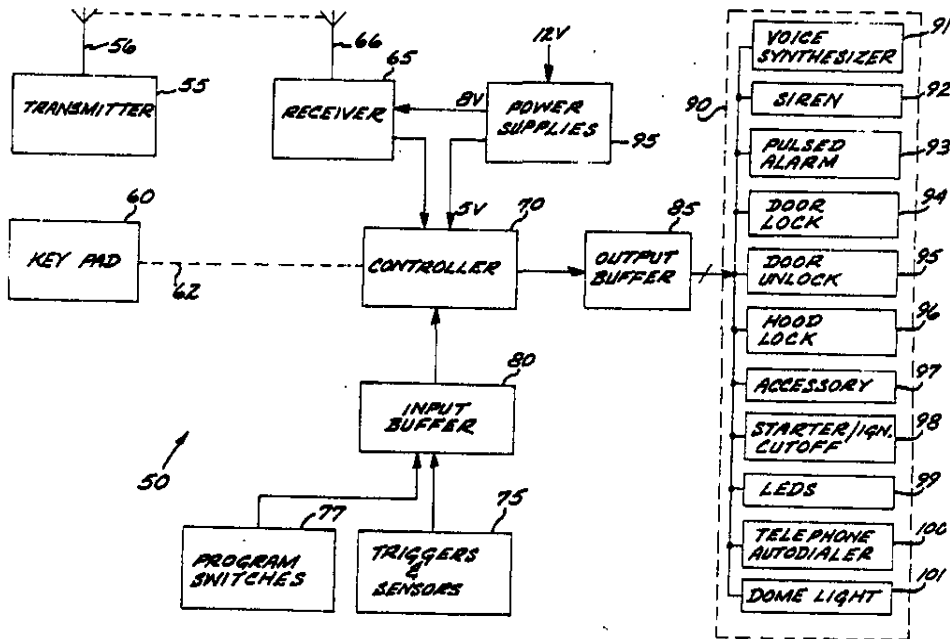
Assistant Examiner—Brian R. Tumm

Attorney, Agent, or Firm—Roberts and Quogue

[57] **ABSTRACT**

A multi-function security system for monitoring access to a protected area such as a vehicle. The system has a self-diagnostic capability for detecting defective sensor or trigger devices and bypassing such devices to allow the system to be armed. The system includes audible and visual message capability for providing an indication when the system is disarmed that an intrusion was attempted and identifying the particular intrusion point. Multiple levels of security are provided by programming the disarming event as either entry of a code via a remote transmitter or entry of the code via the transmitter and then entry of an authorization code manually via a key pad. Other features include a reset feature activating the alarm when power is removed and restored unless a predetermined switch is active, programmable door lock and unlock signals to adapt the system to a particular power door locking and unlocking system, programmability of the alarm siren code and duration, automatic activation of the vehicle courtesy light when the system is disarmed, selective disabling of the system audible indications of arming and disarming, and programmable sensor or trigger polarity.

67 Claims, 46 Drawing Sheets

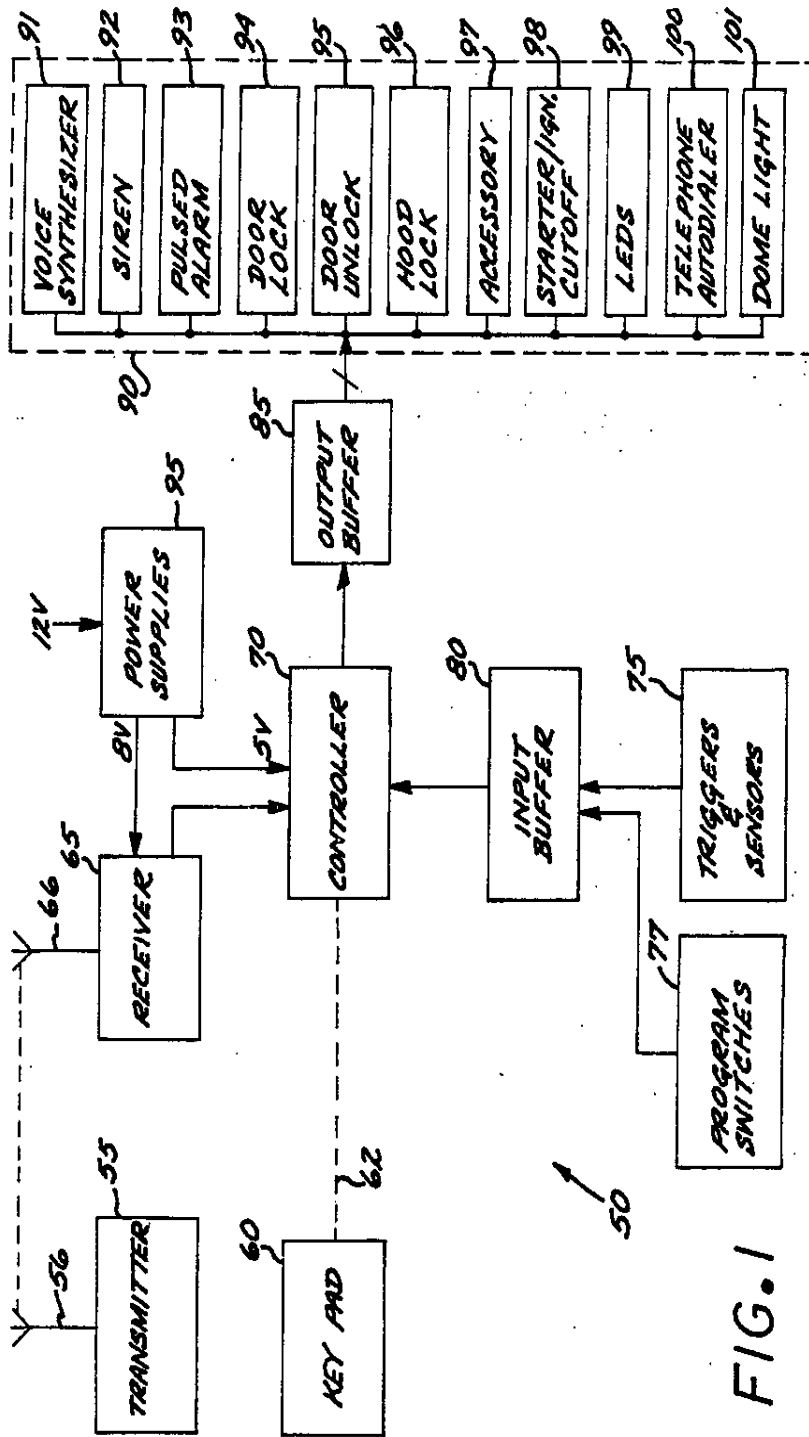


U.S. Patent

Dec. 12, 1989

Sheet 1 of 46

4,887,064



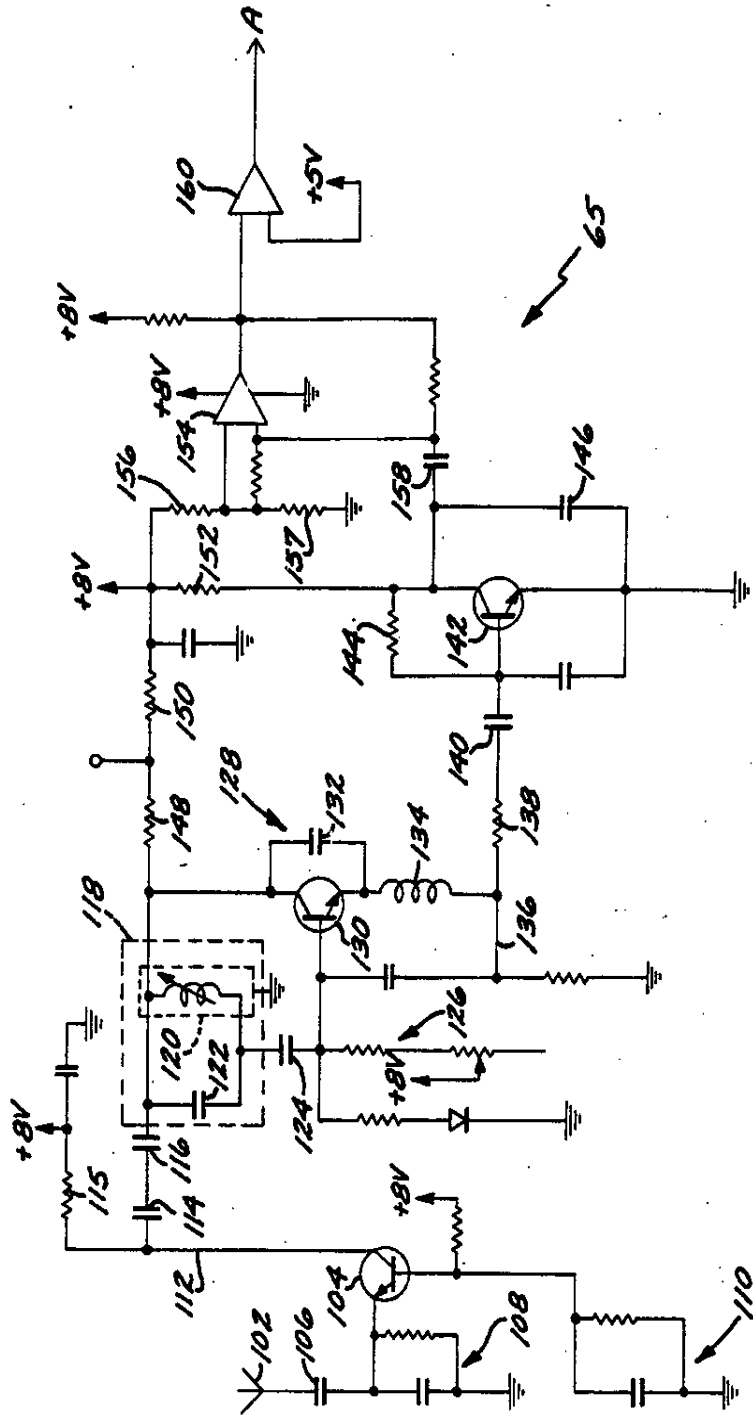


FIG. 2

U.S. Patent

Dec. 12, 1989

Sheet 3 of 46

4,887,064

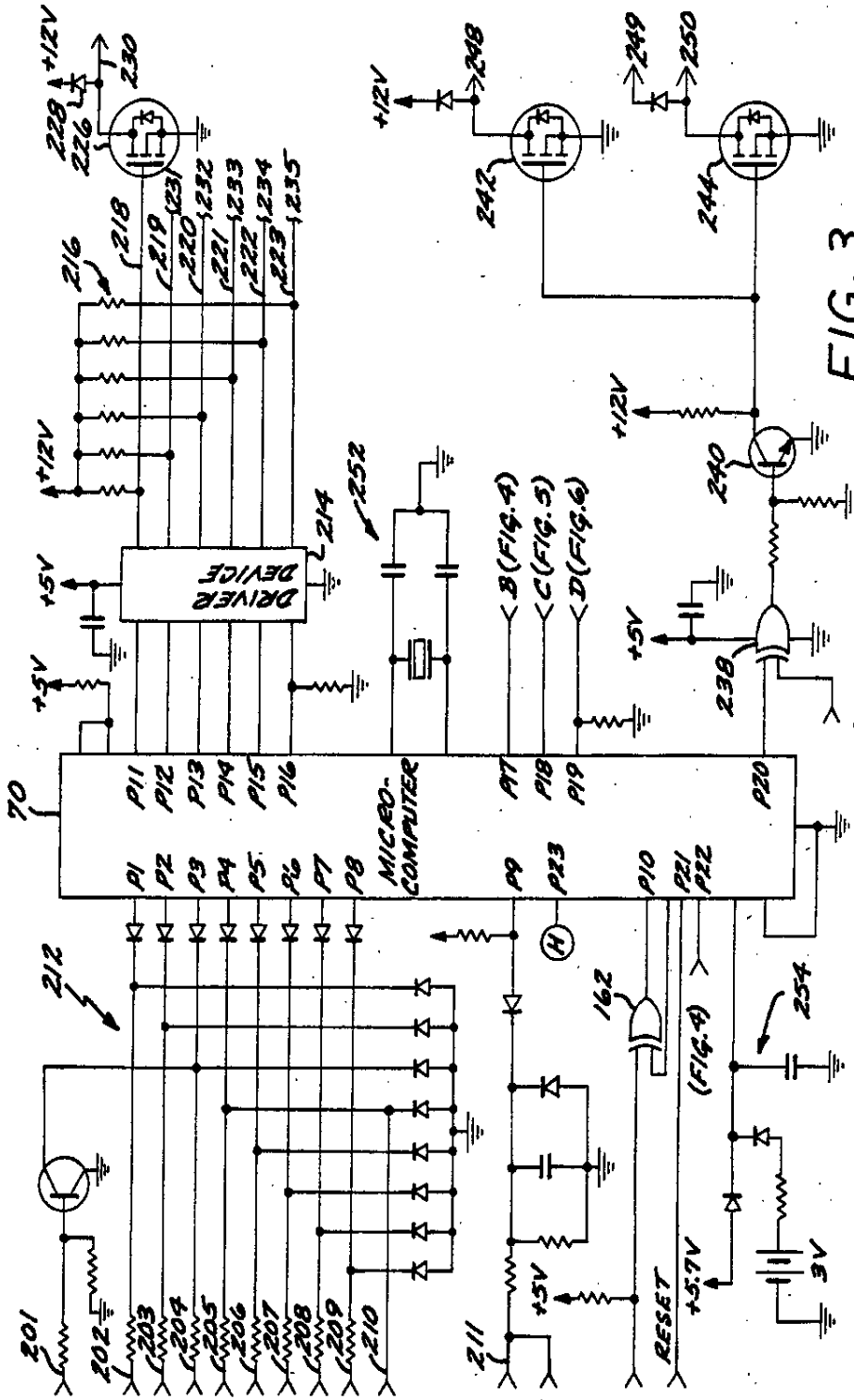


FIG. 3

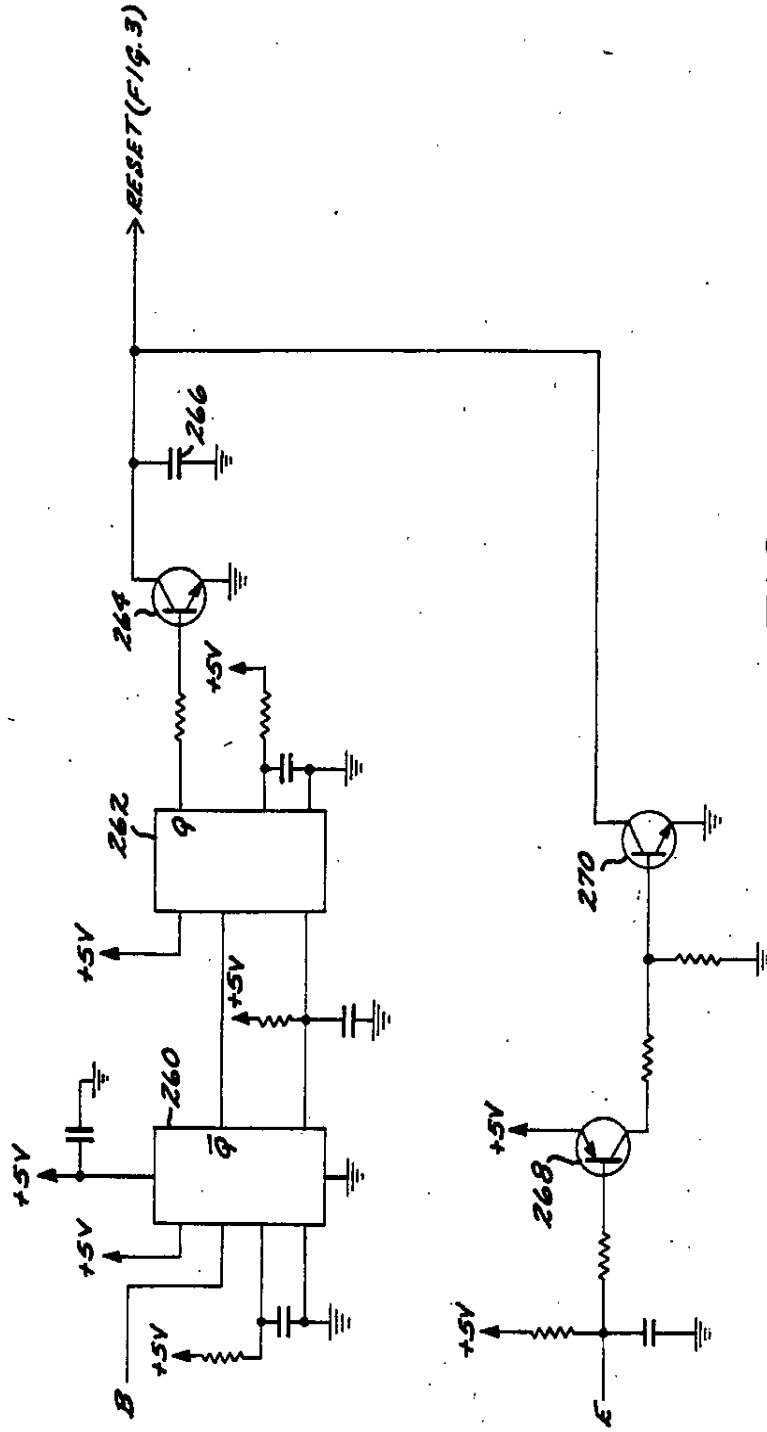


FIG. 4

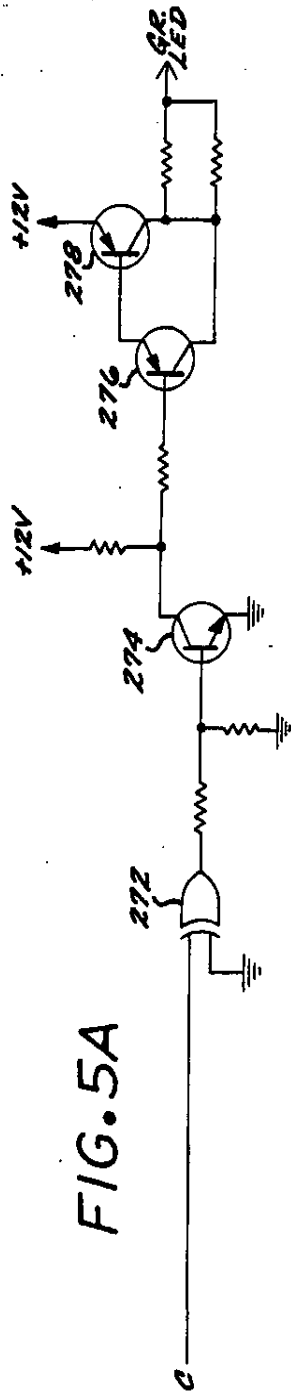


FIG. 5A

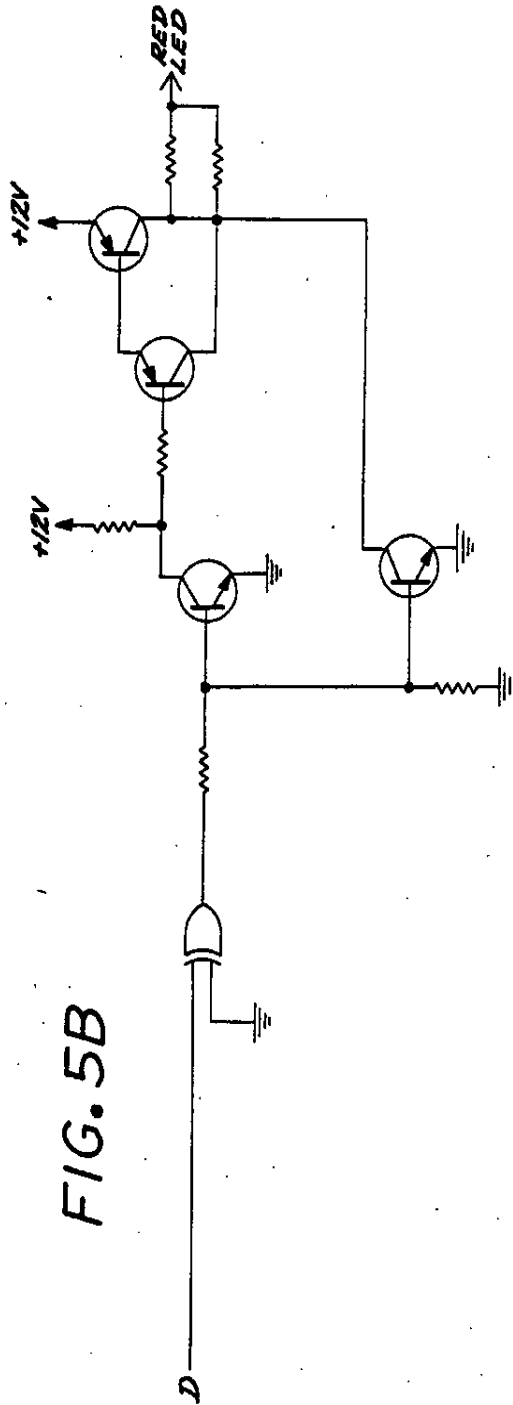


FIG. 5B

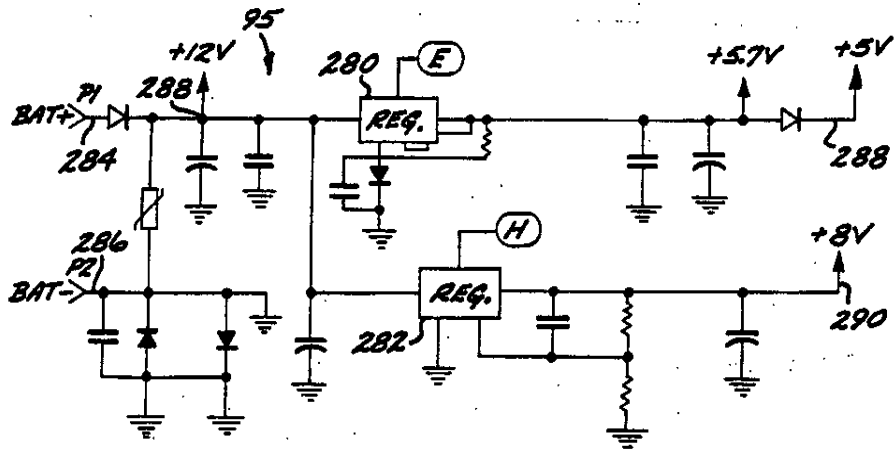


FIG. 6

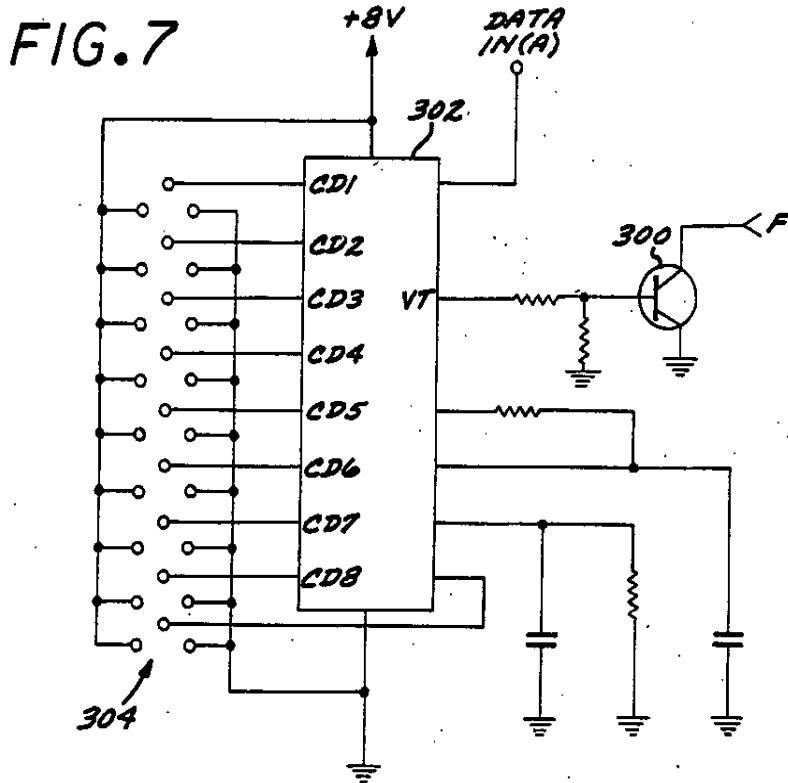


FIG. 7

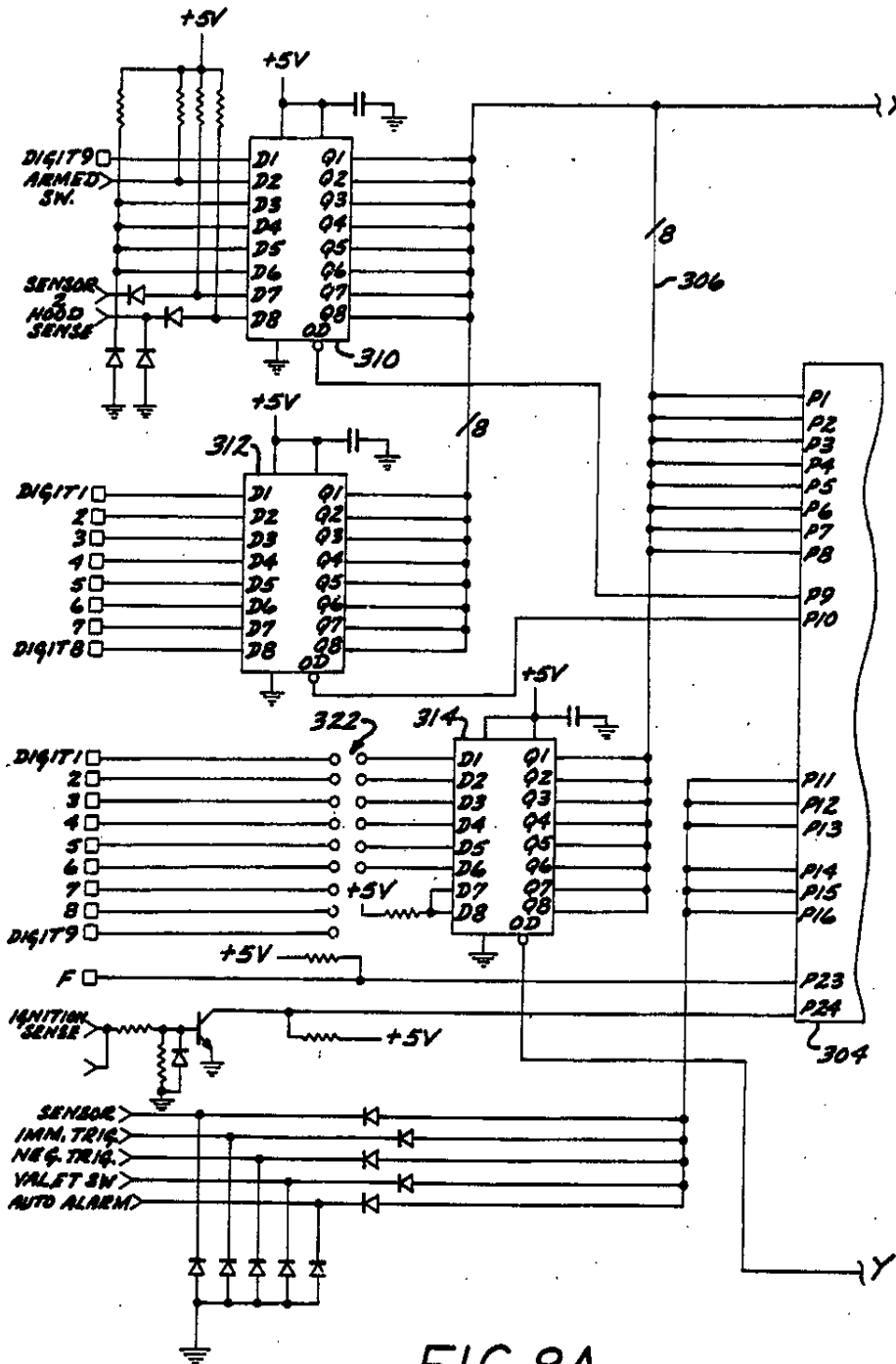


FIG. 8A

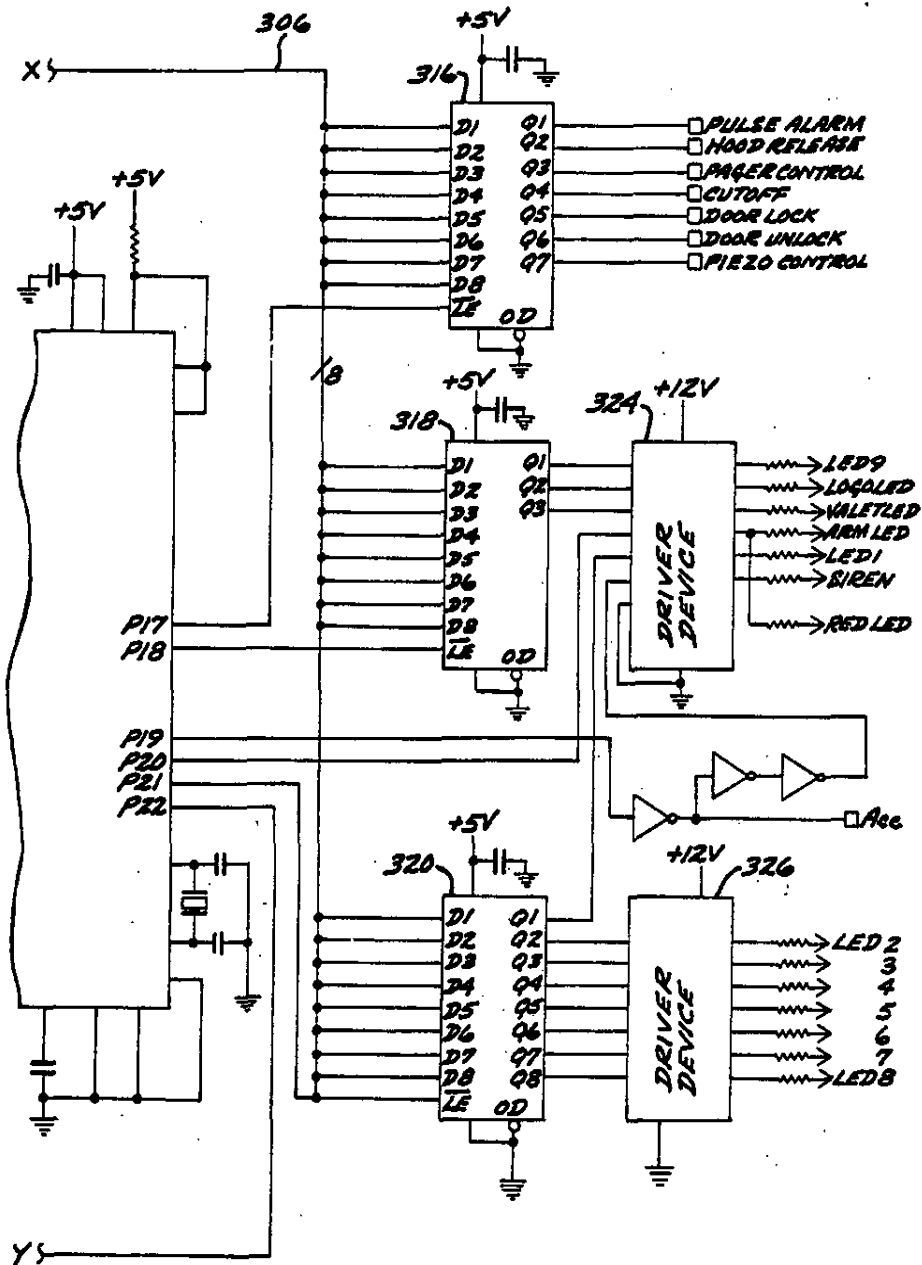


FIG. 8B

FIG. 9

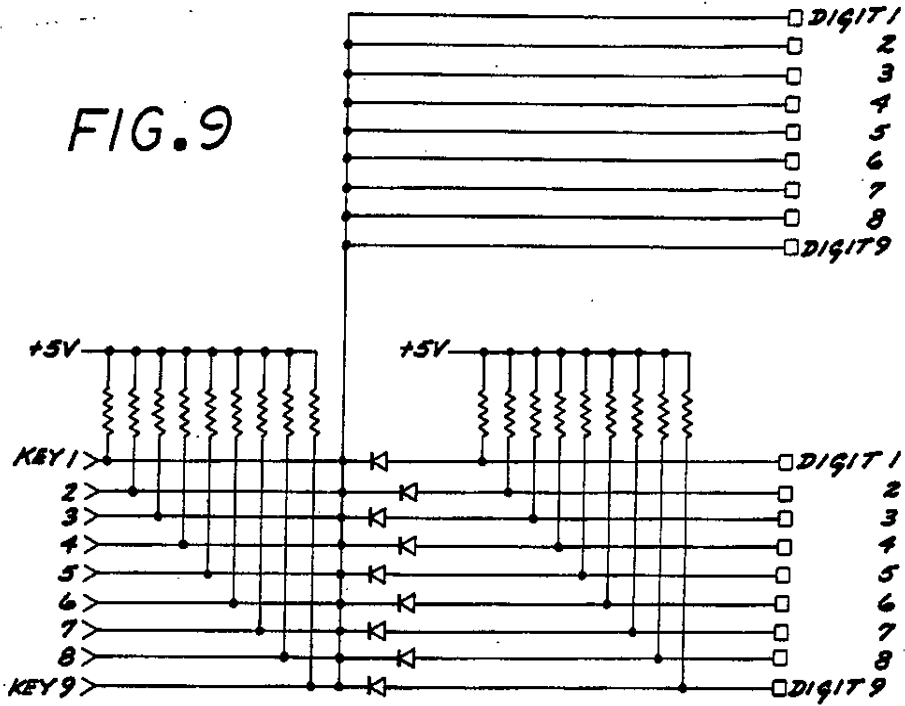
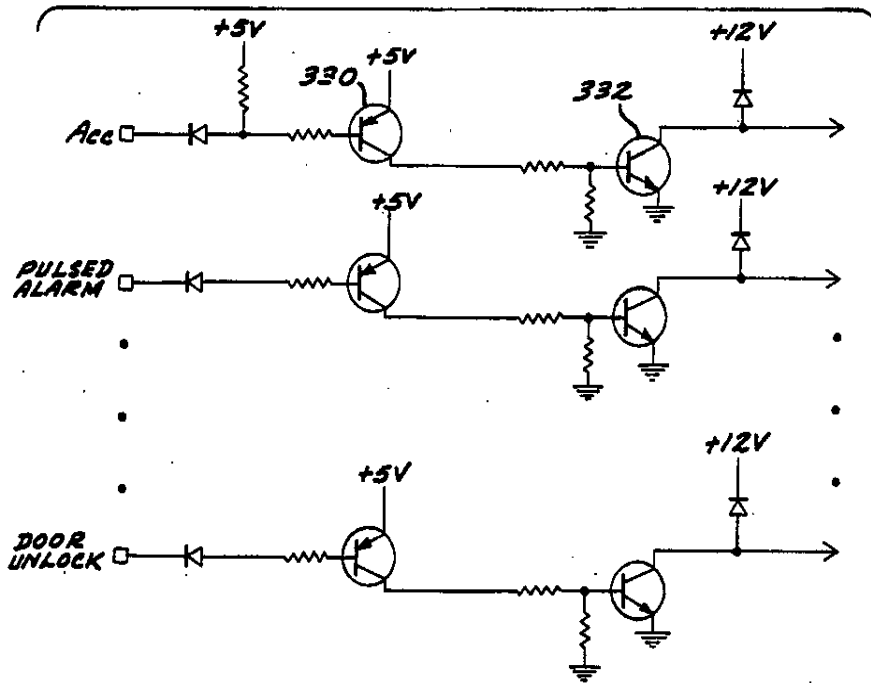


FIG. 10



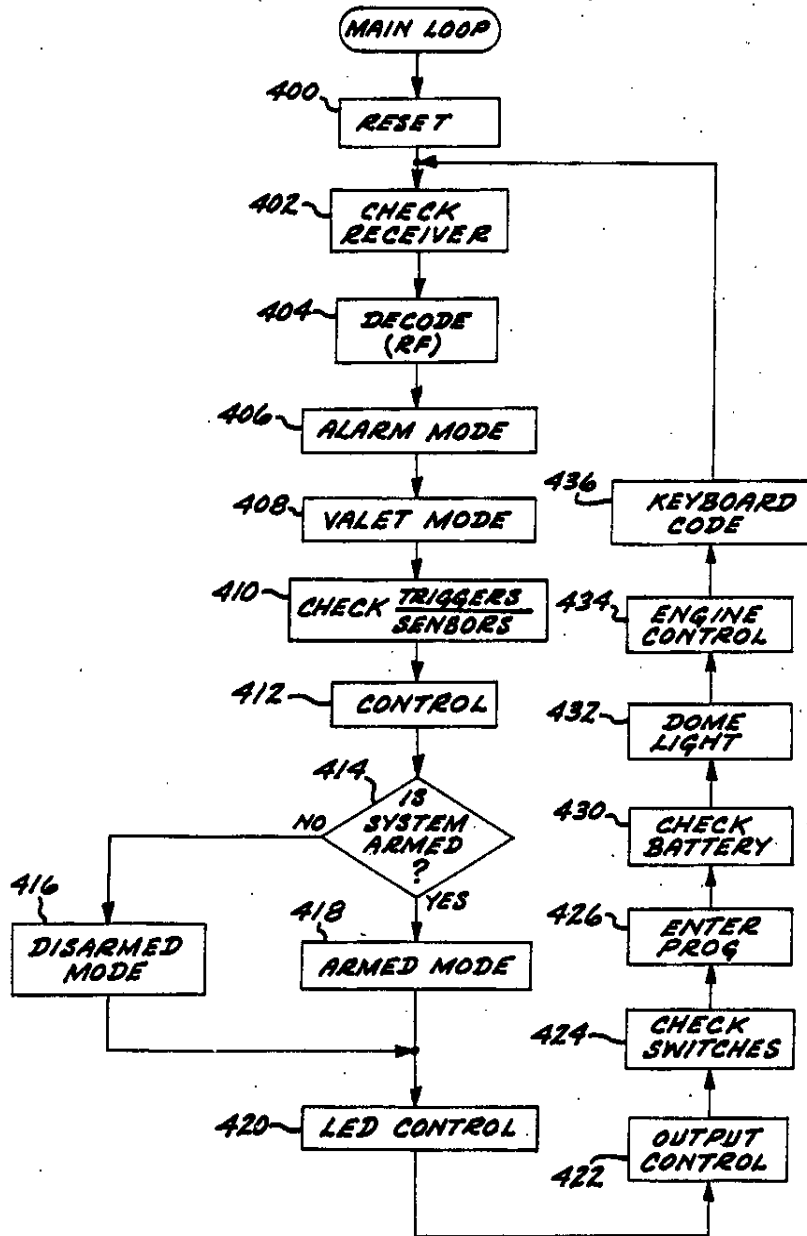


FIG. 11

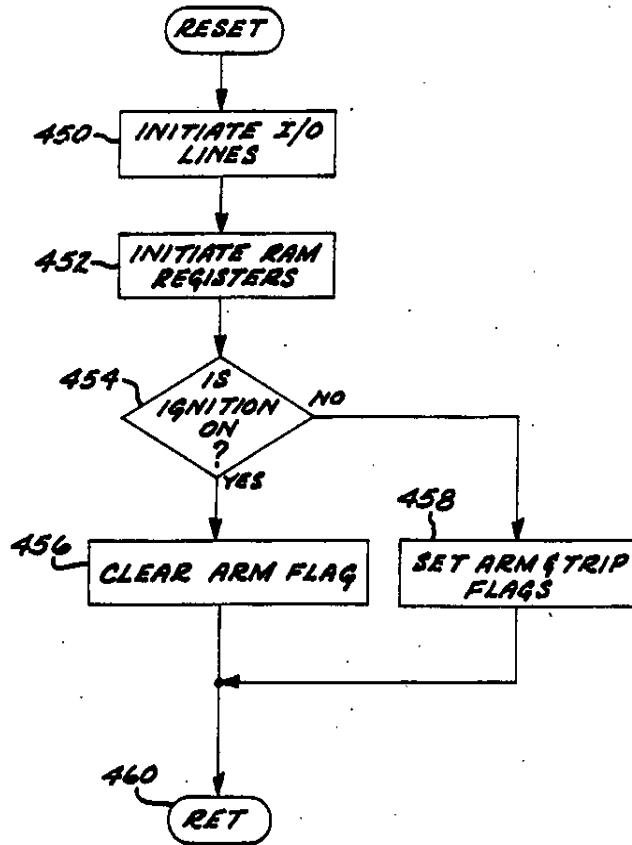


FIG. 12

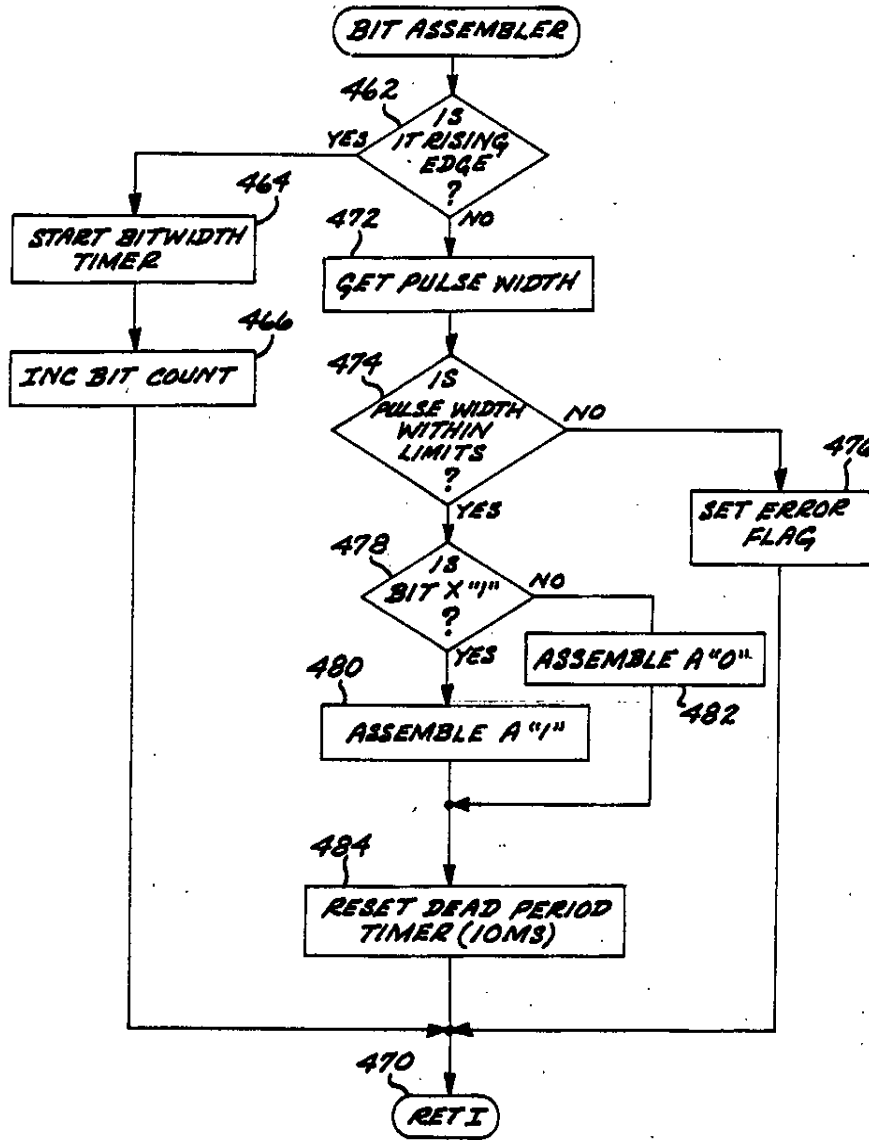


FIG. 13A

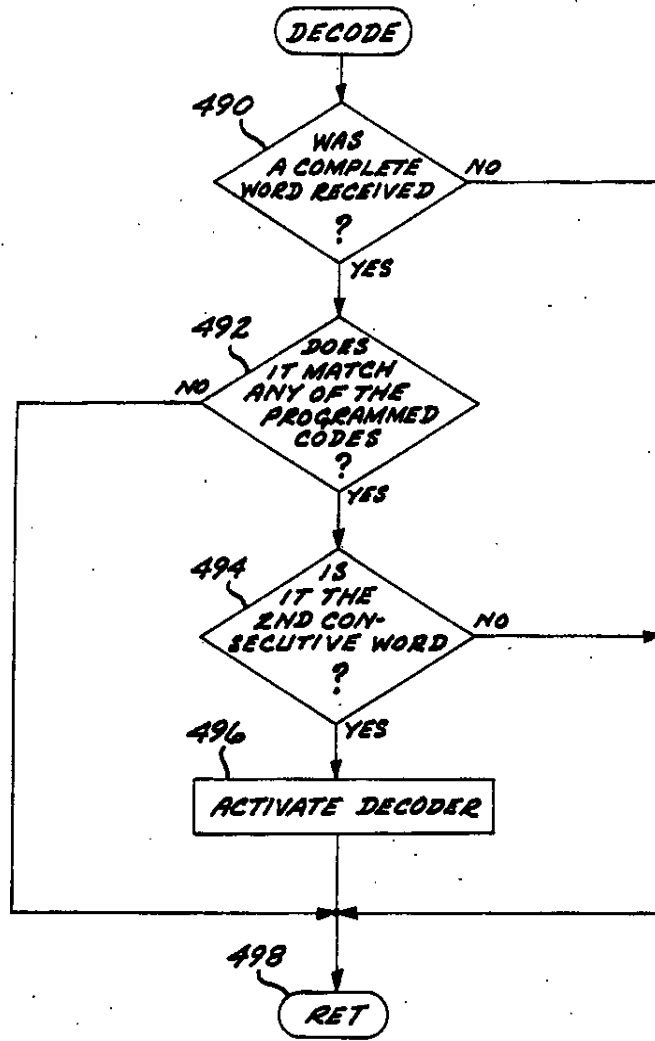


FIG. 13B

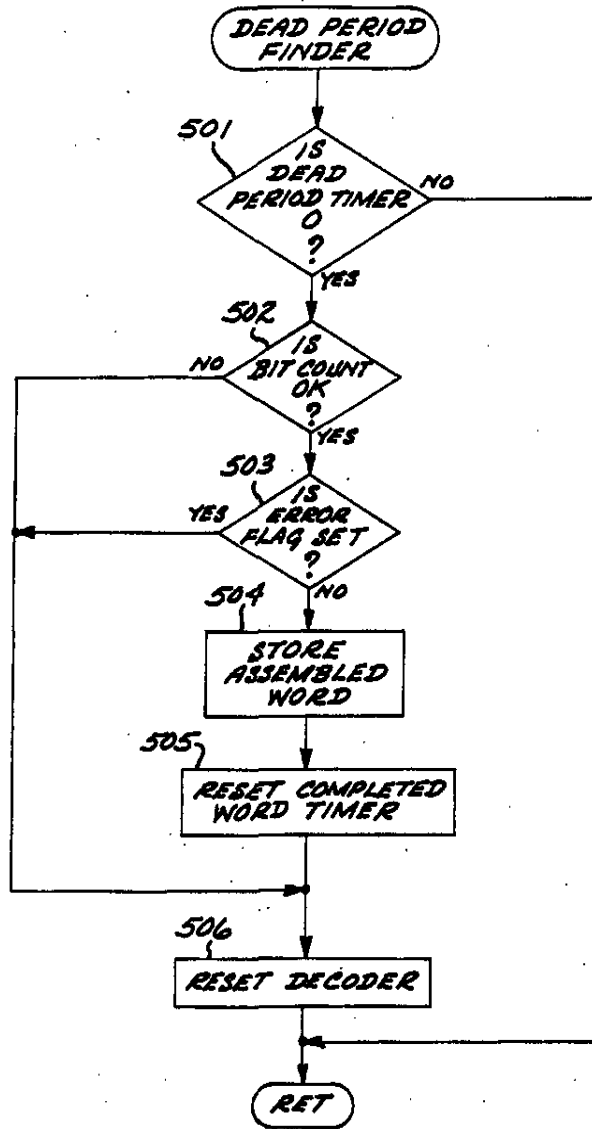


FIG. 13C

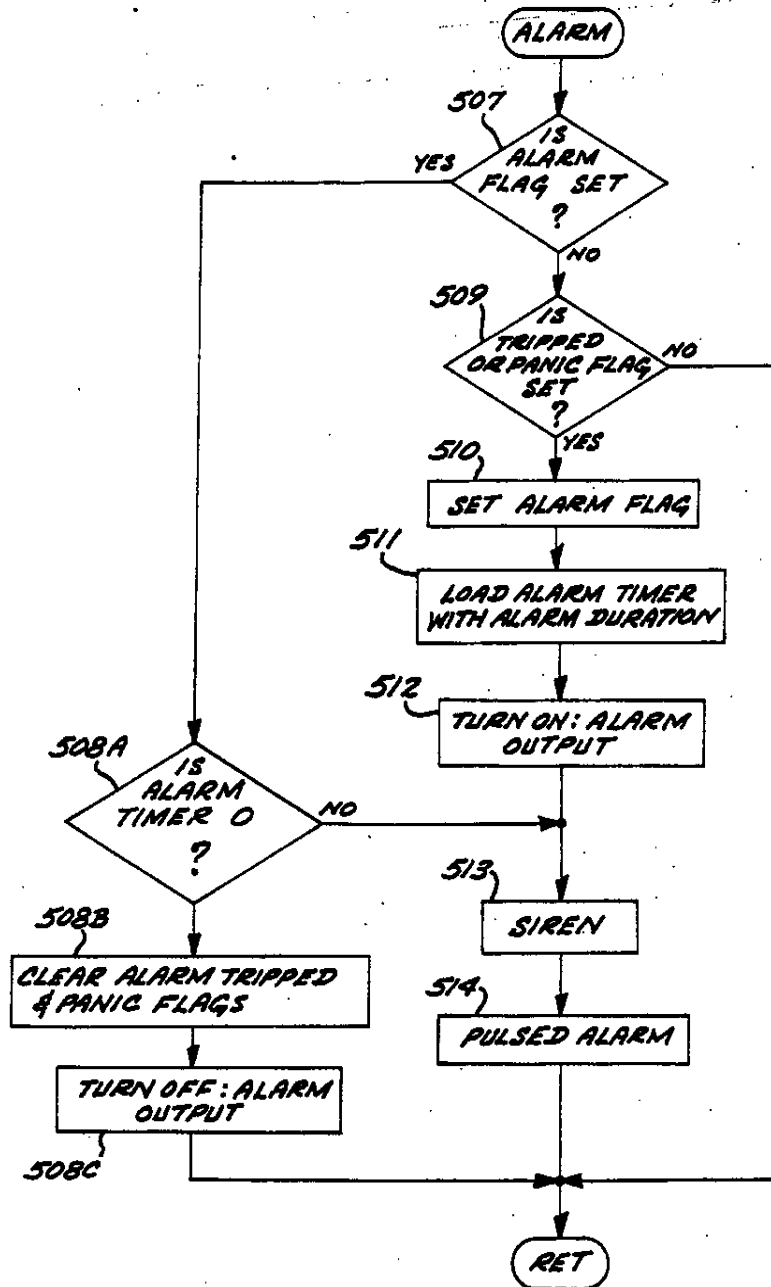


FIG. 14A

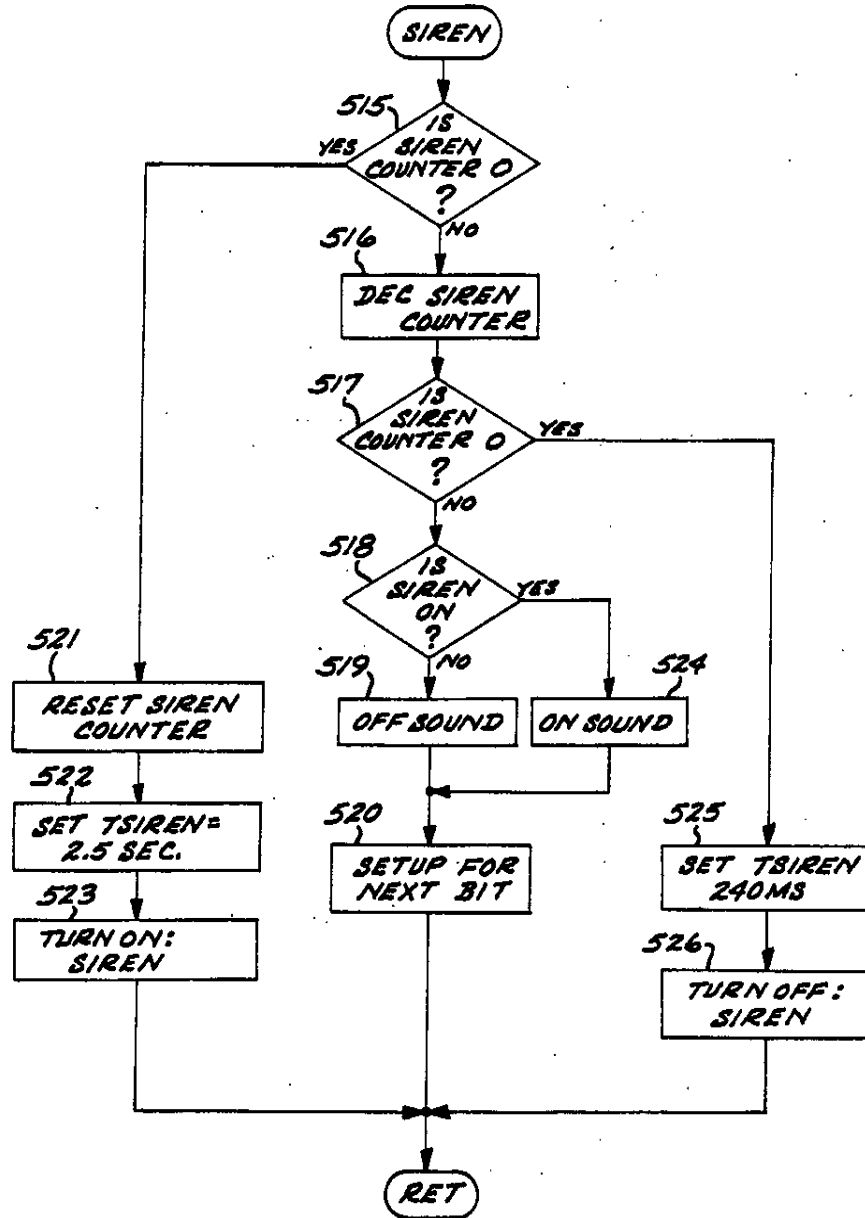


FIG. 14B

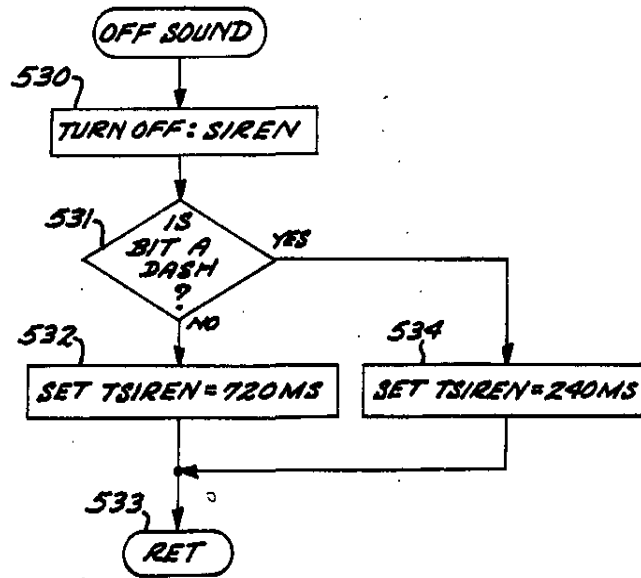


FIG. 14C

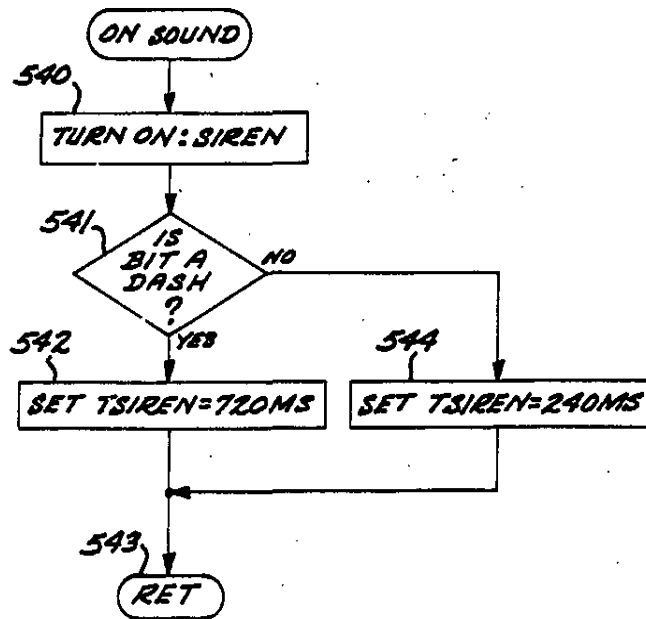


FIG. 14D

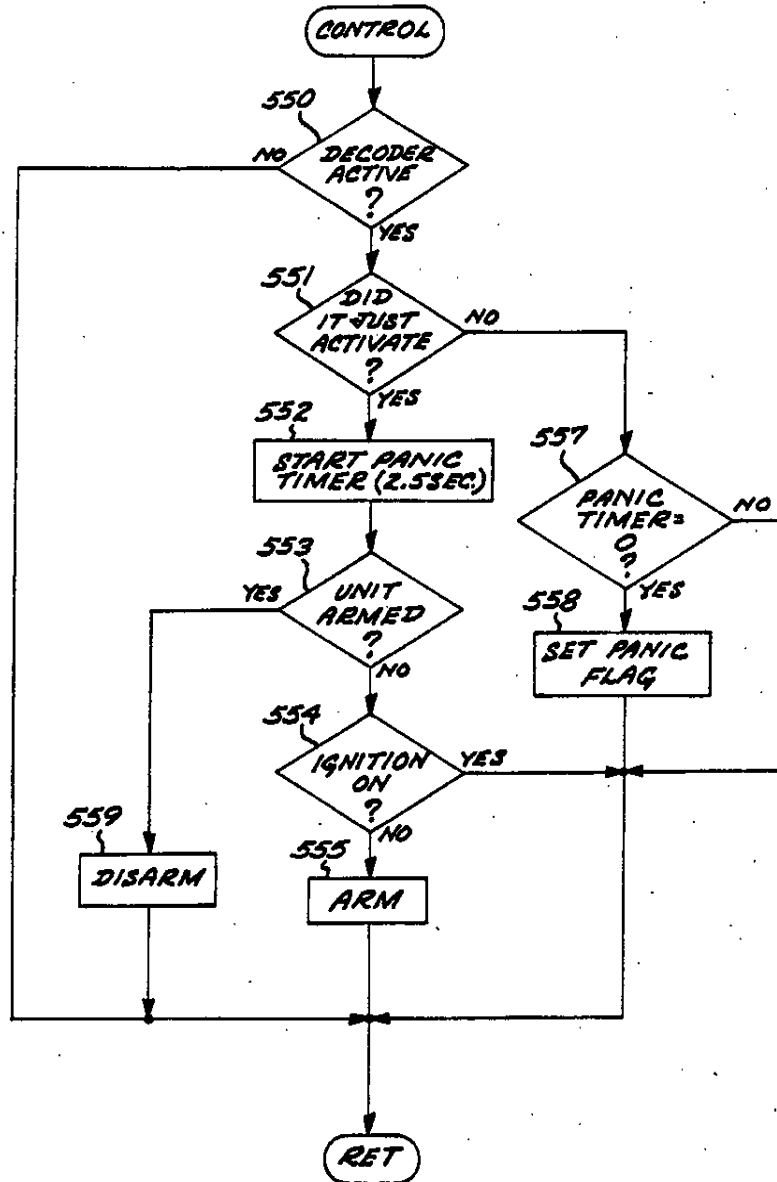


FIG. 15A

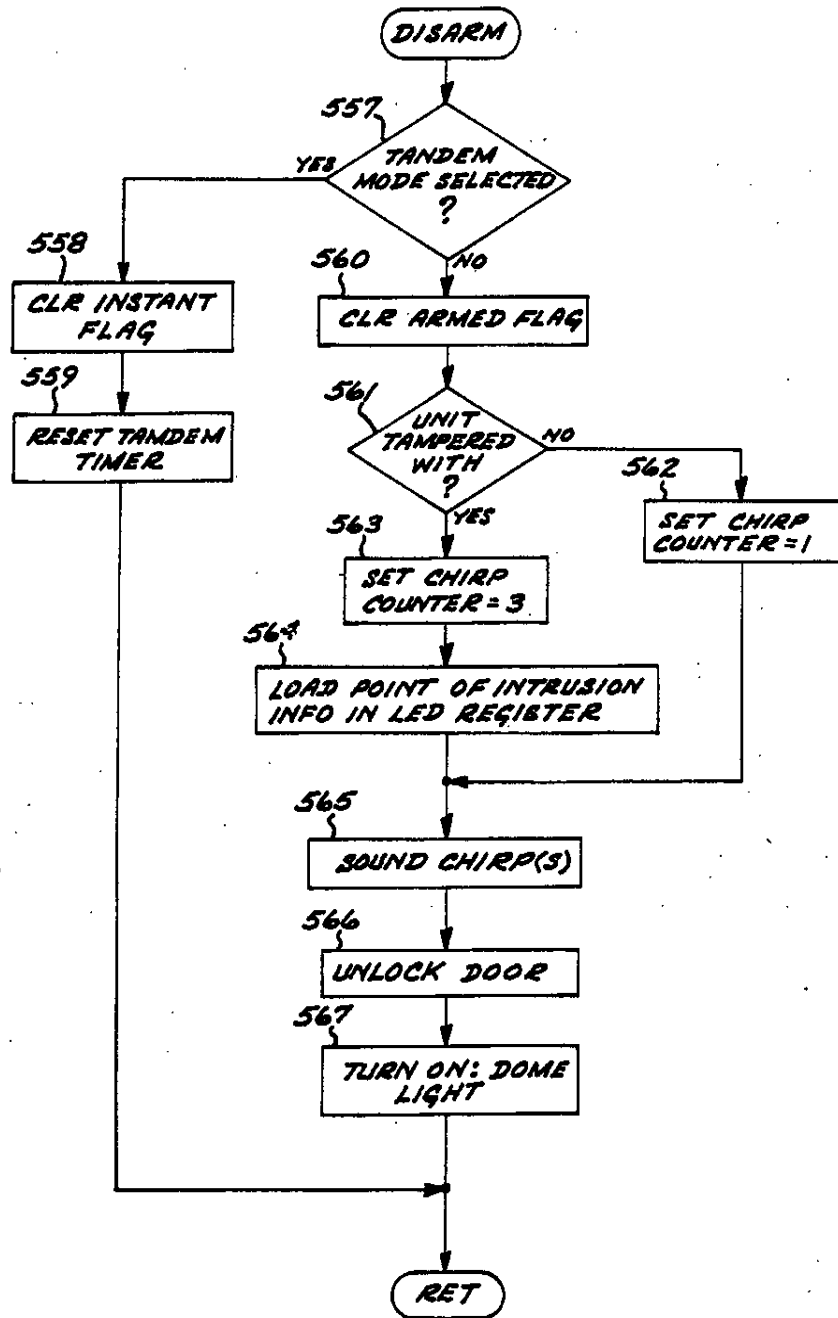


FIG. 15B

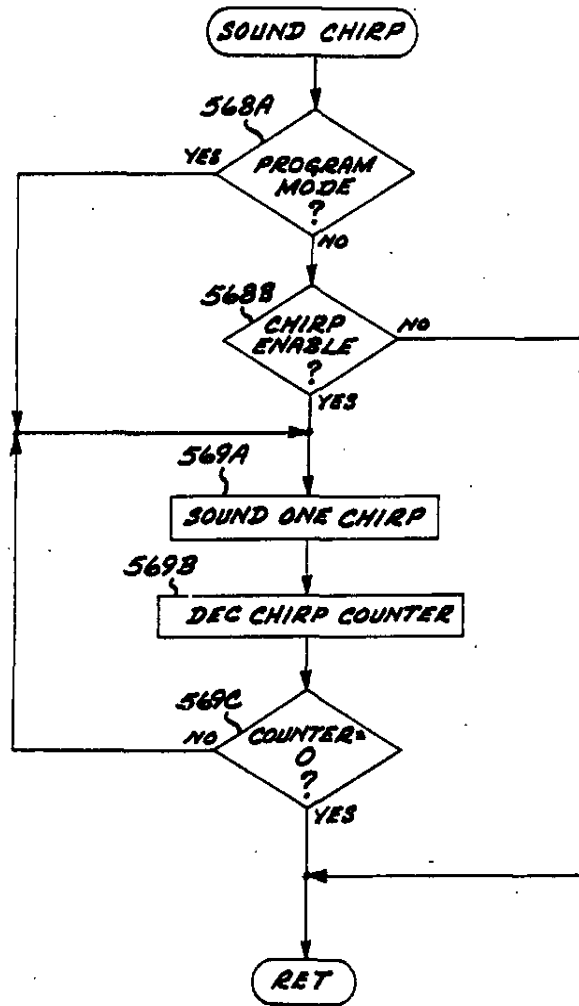


FIG.15C

U.S. Patent

Dec. 12, 1989

Sheet 21 of 46

4,887,064

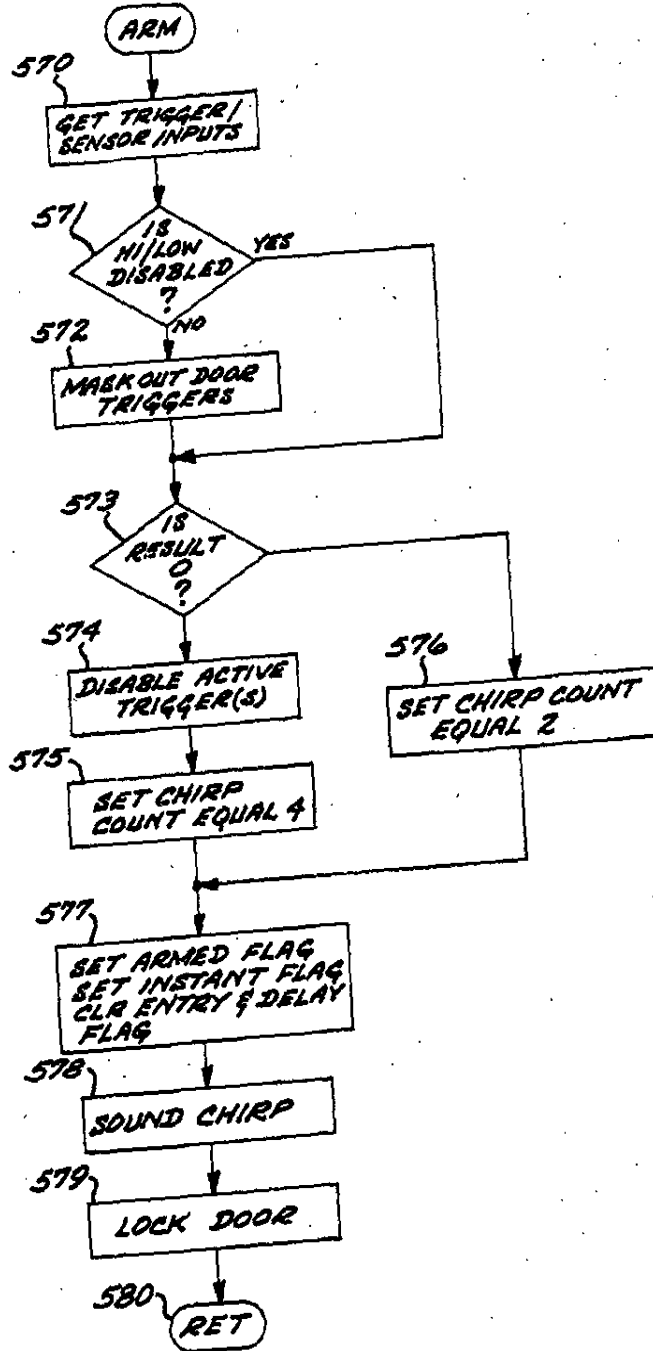


FIG. 15D

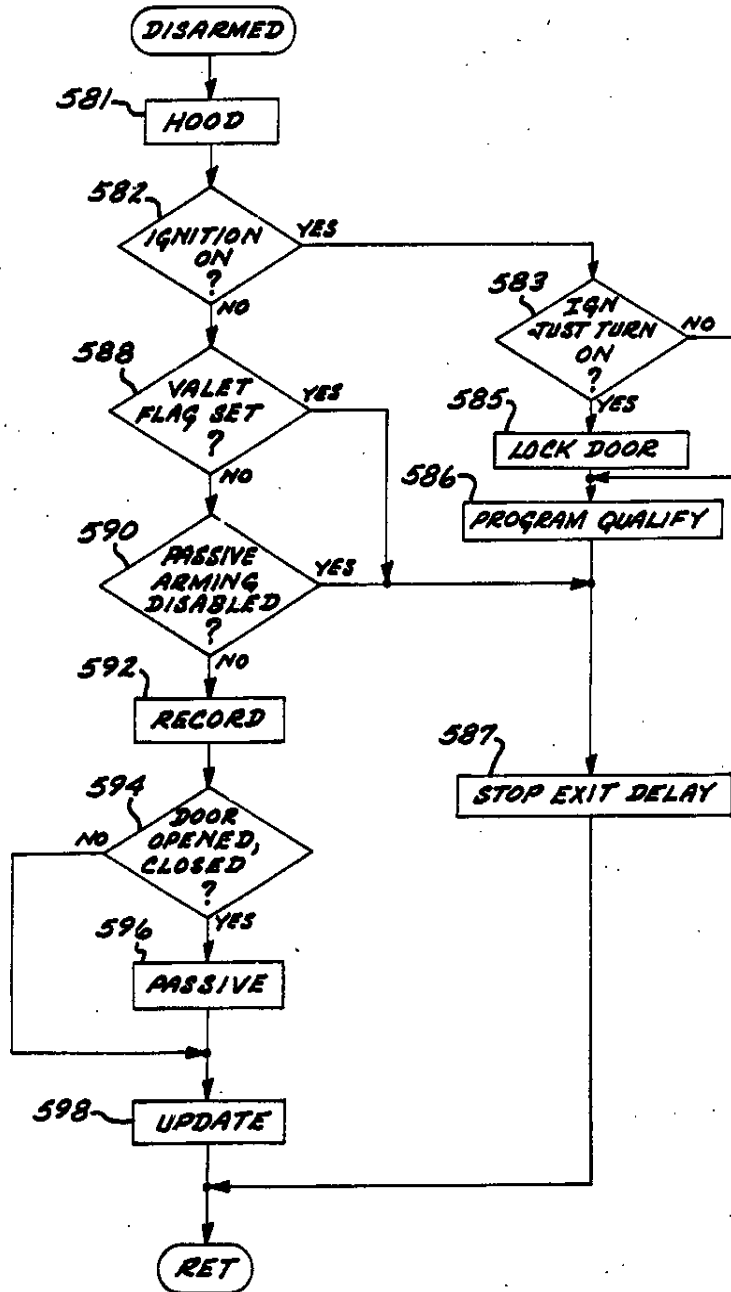


FIG. 16A

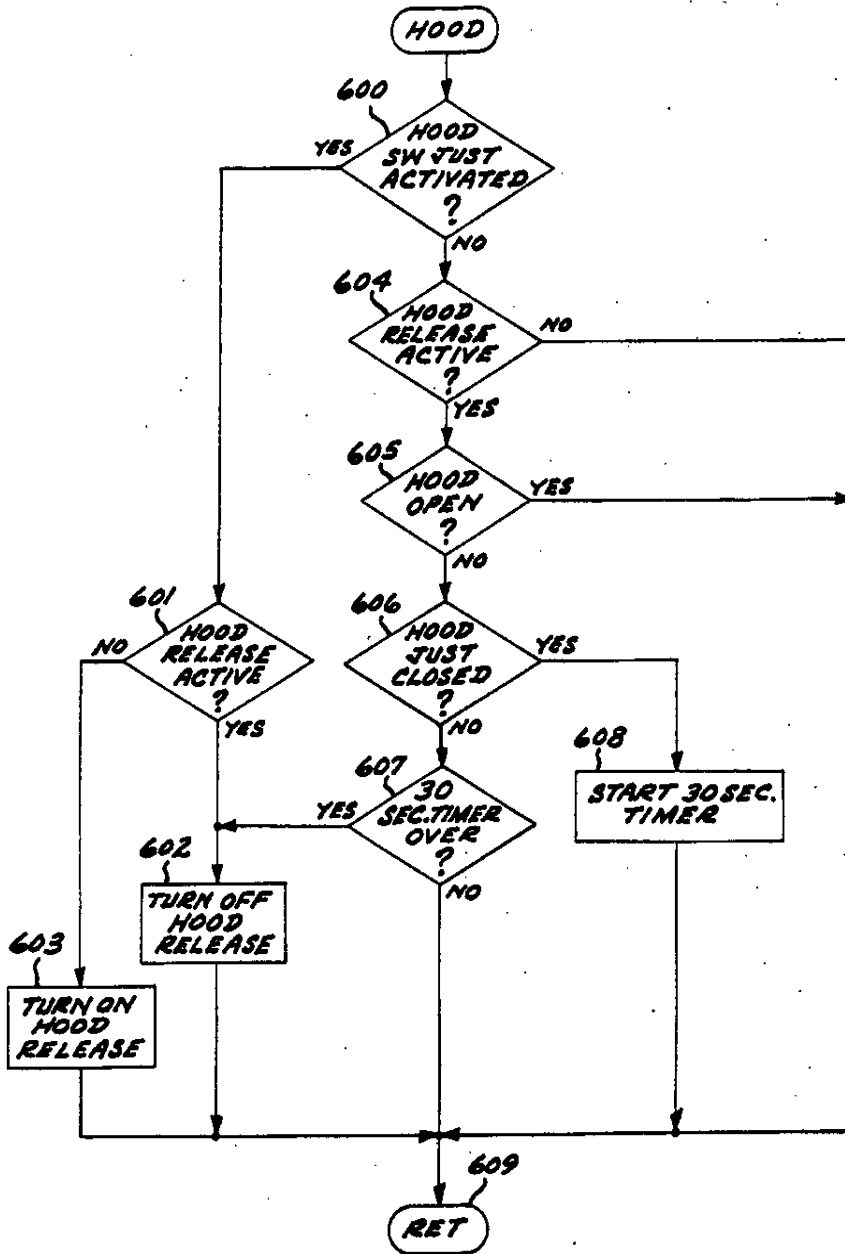


FIG. 16B

FIG. 16C

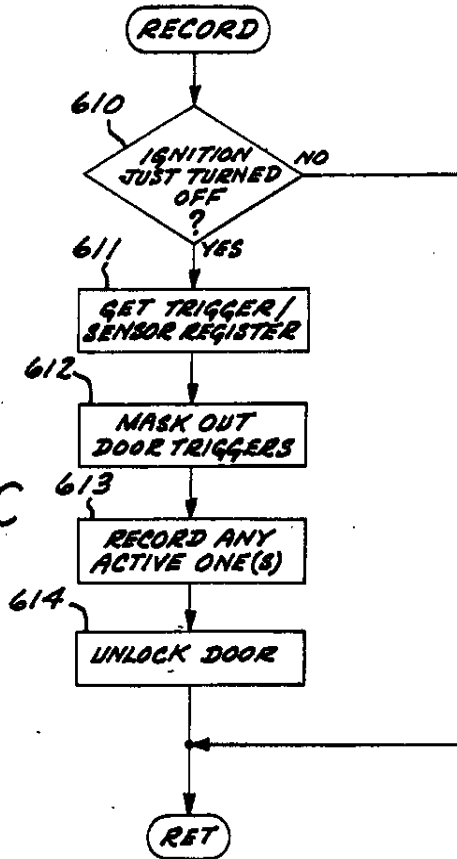
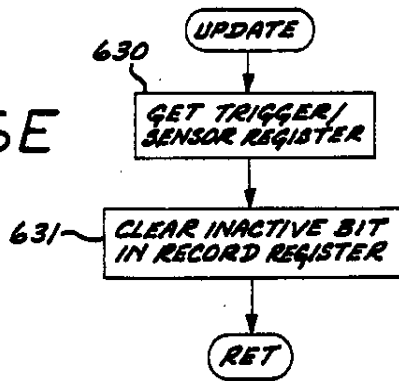


FIG. 16E



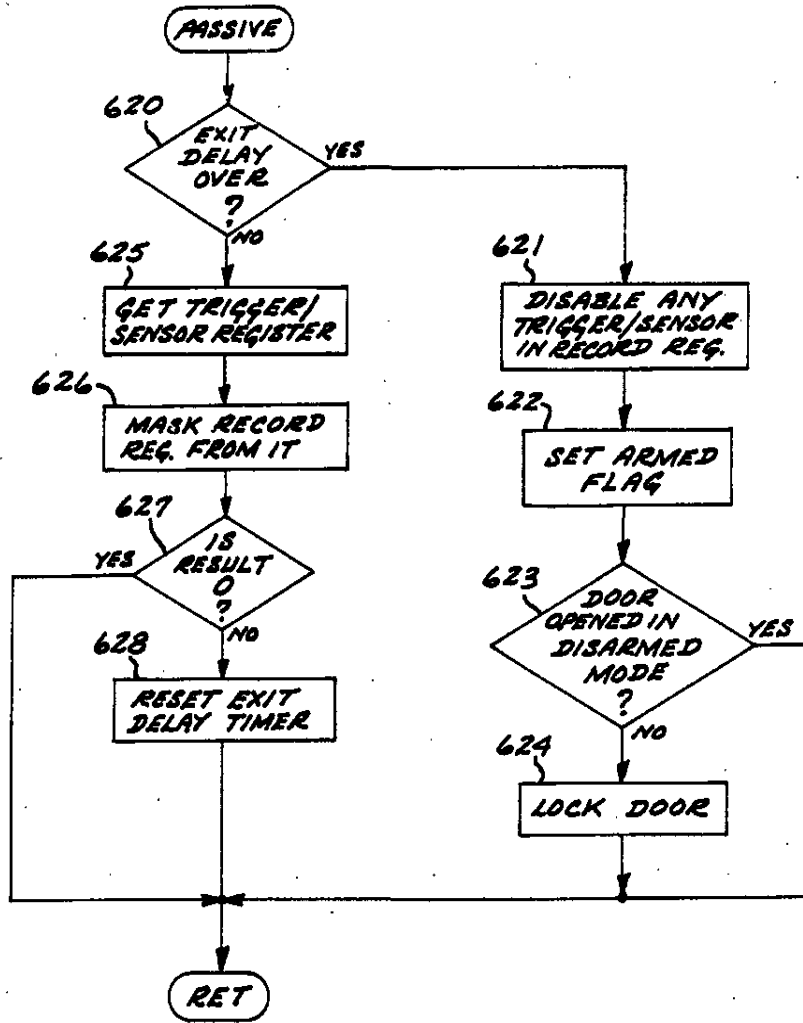


FIG. 16D

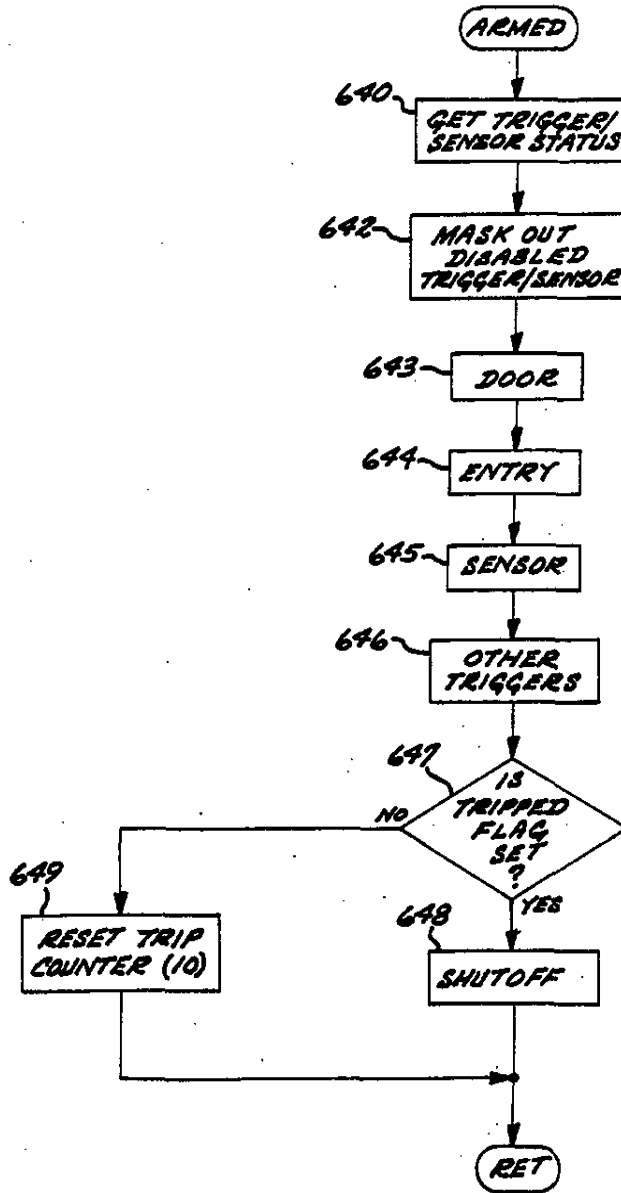


FIG. 17A

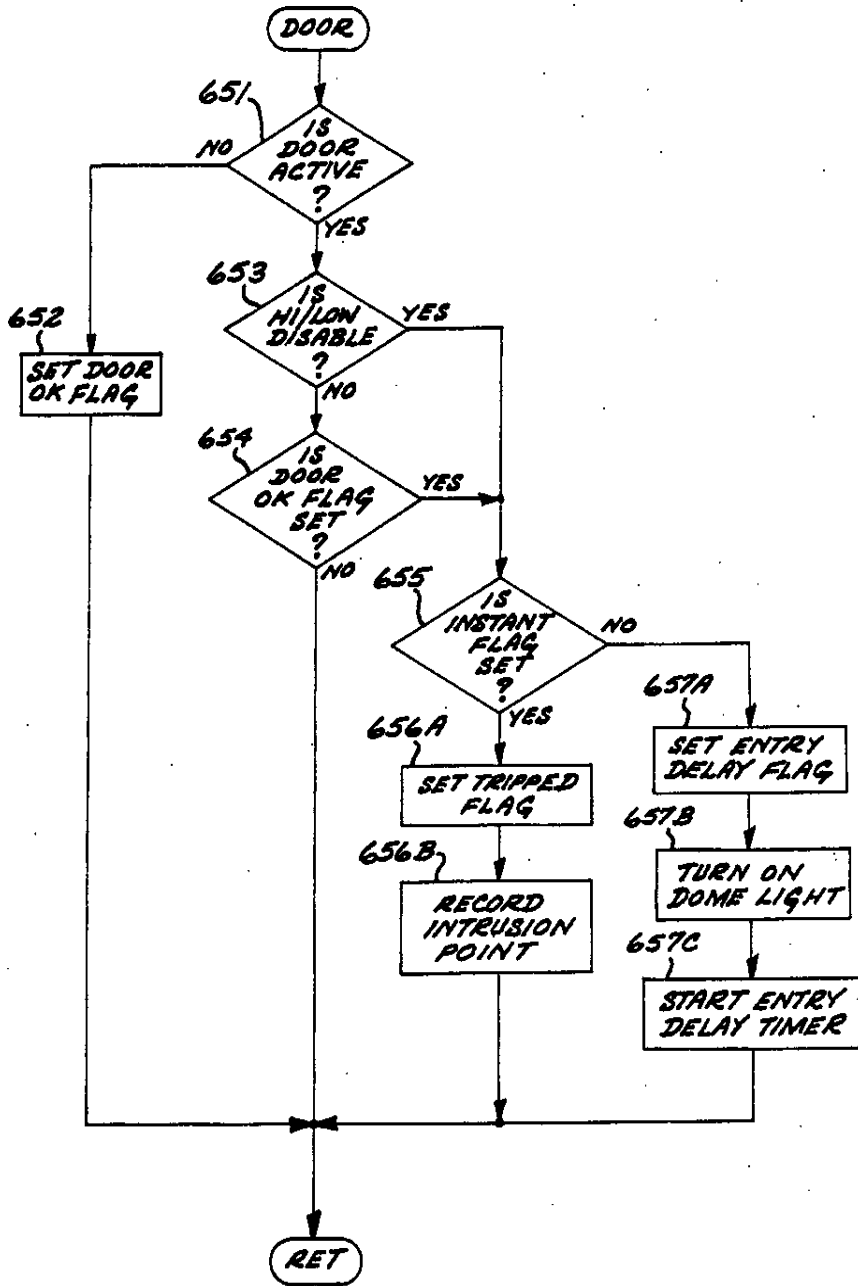


FIG. 17B

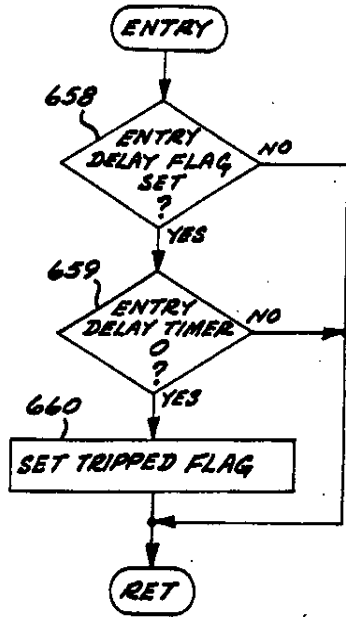


FIG. 17C

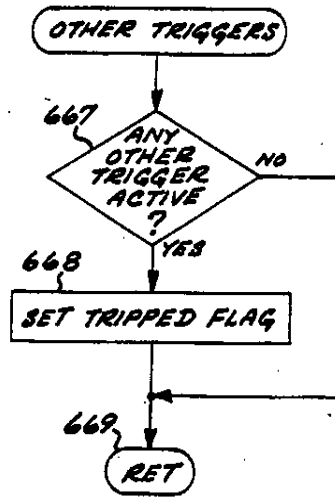


FIG. 17E

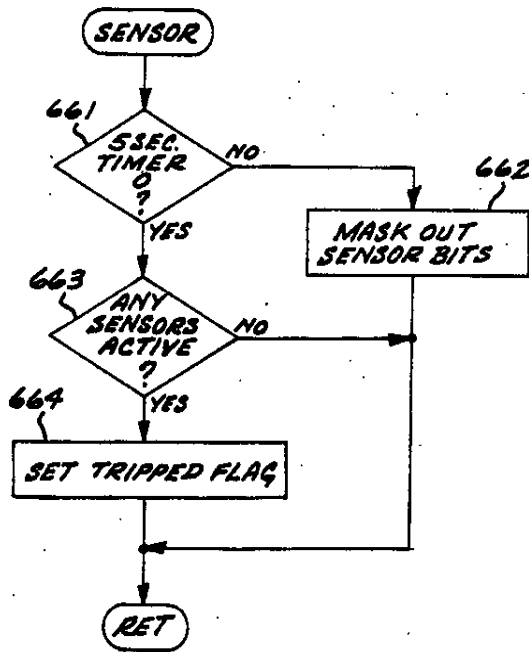


FIG. 17D

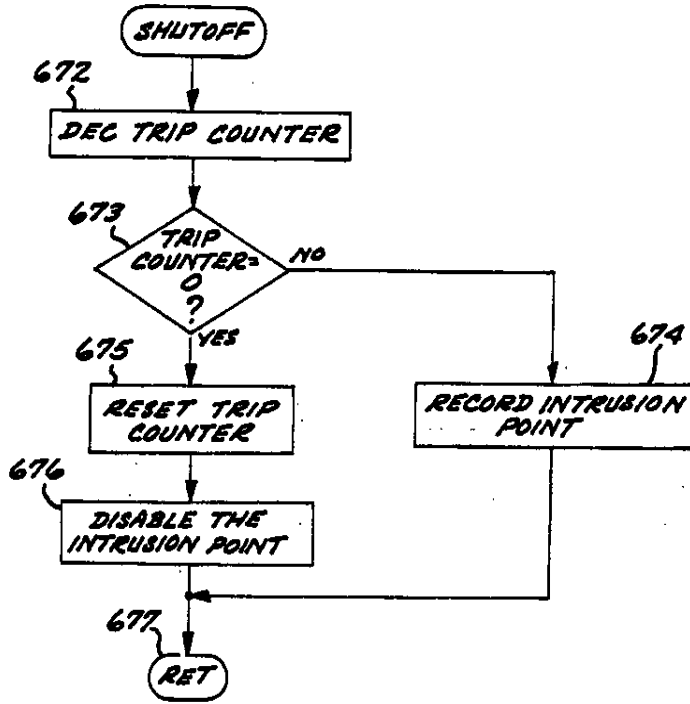


FIG. 17F

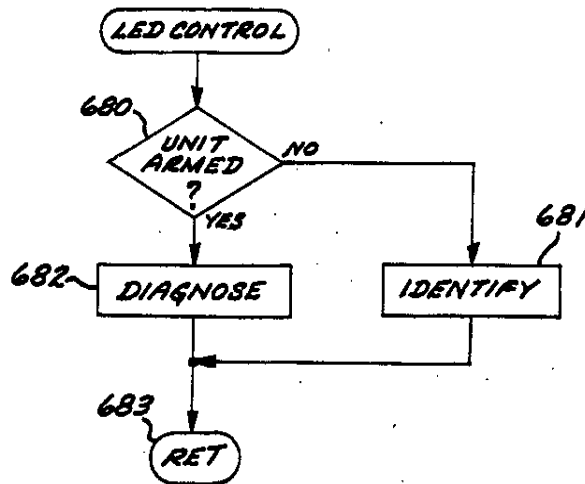


FIG. 18A

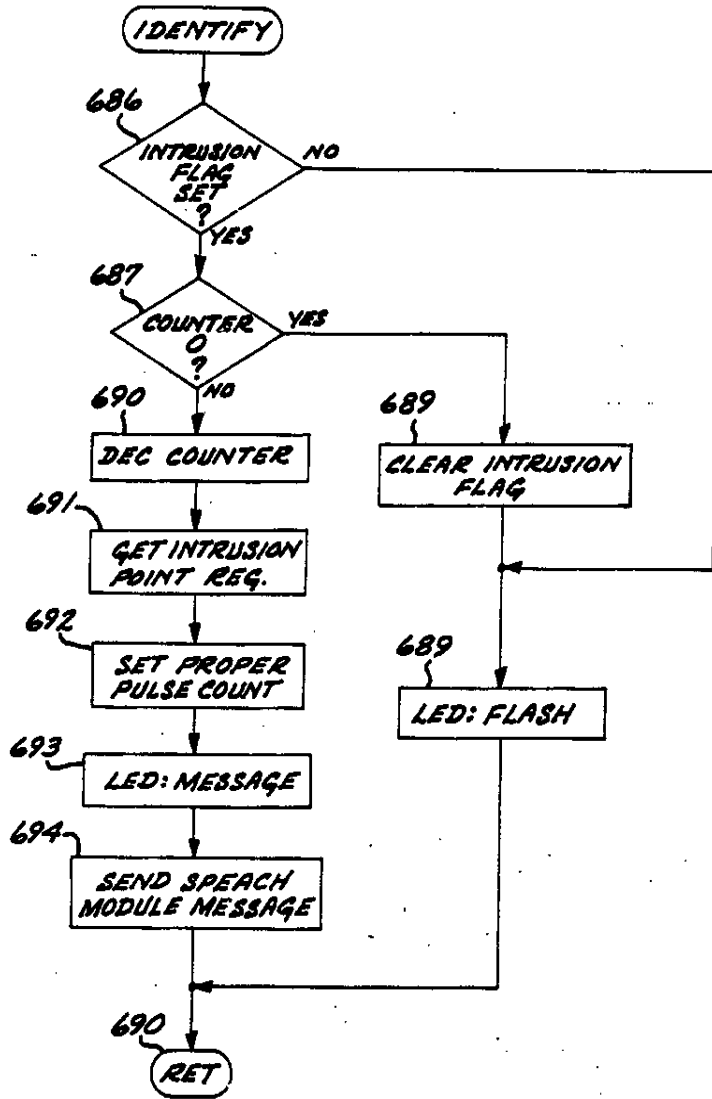


FIG. 18B

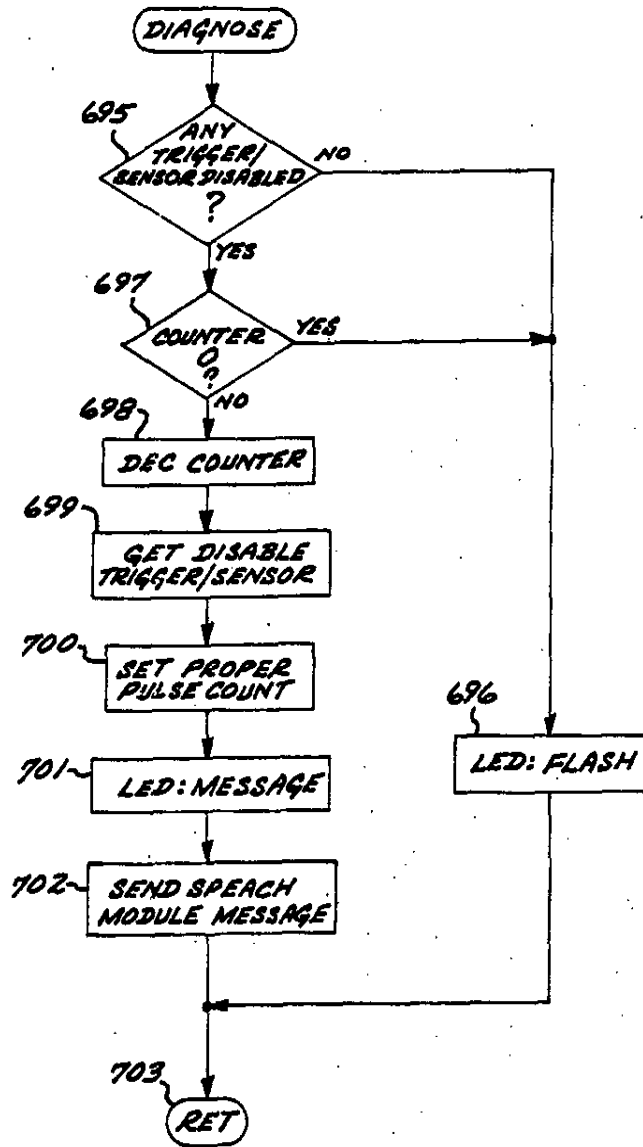


FIG. 18C

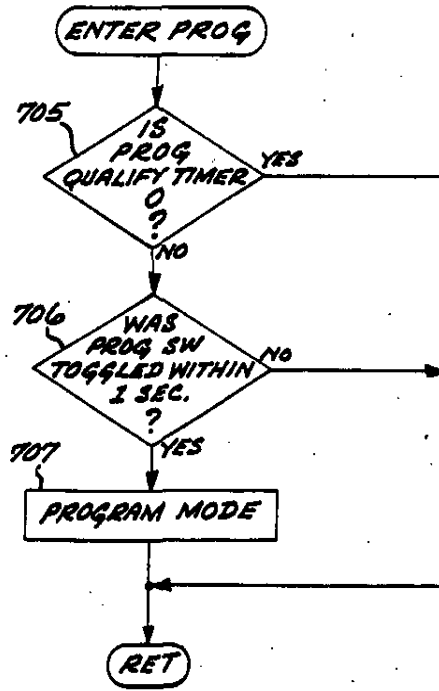
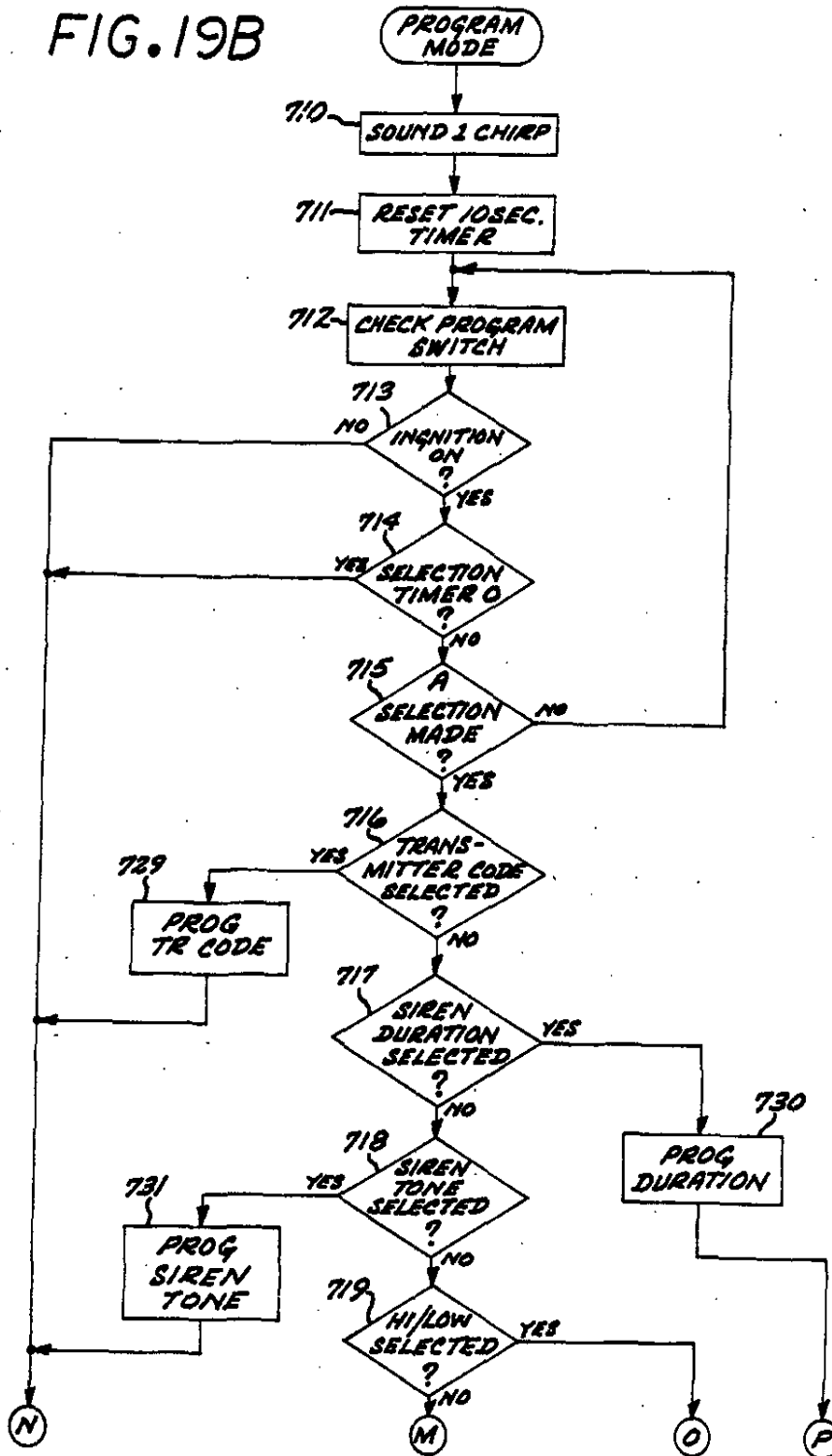


FIG. 19A

FIG. 19B



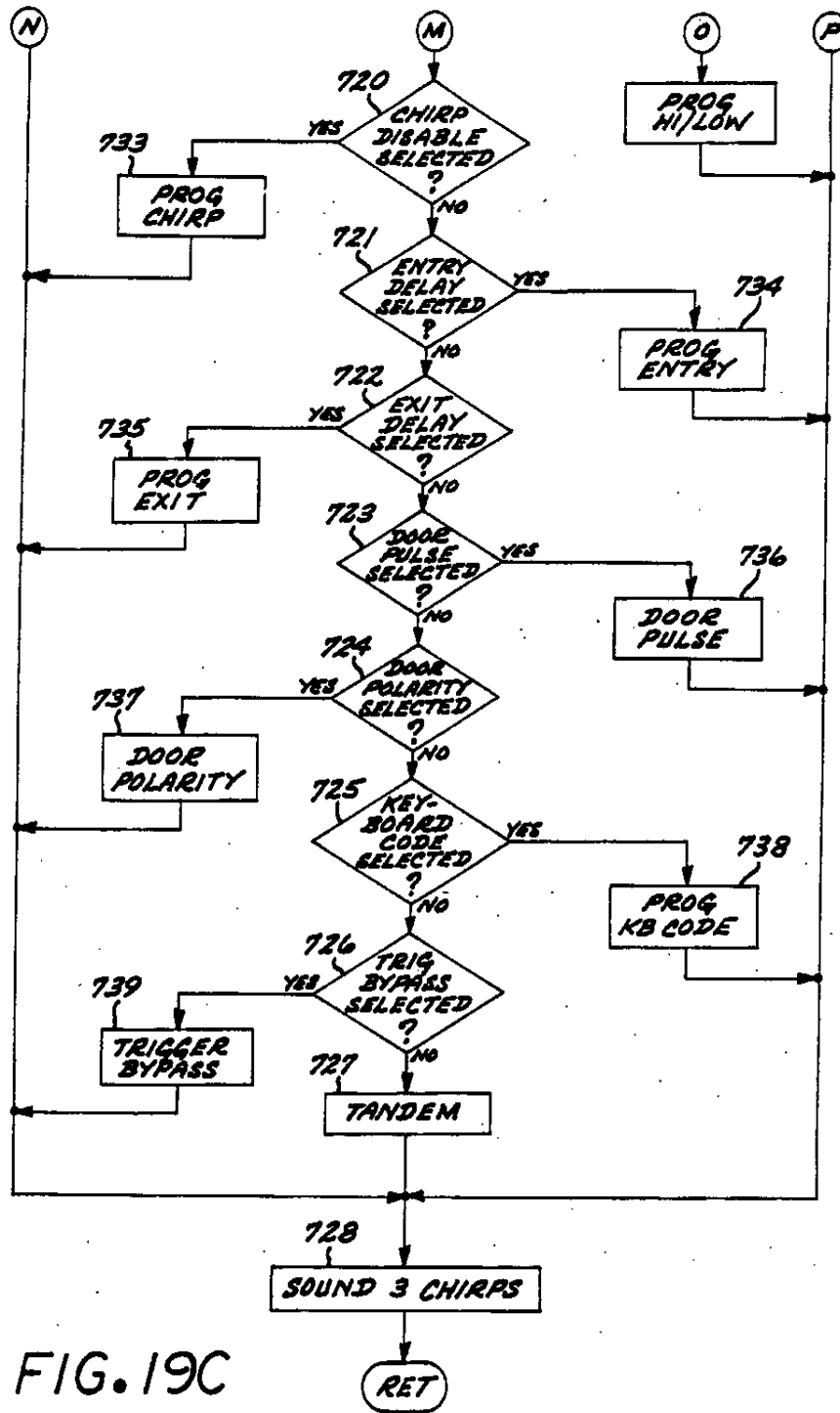


FIG. 19C

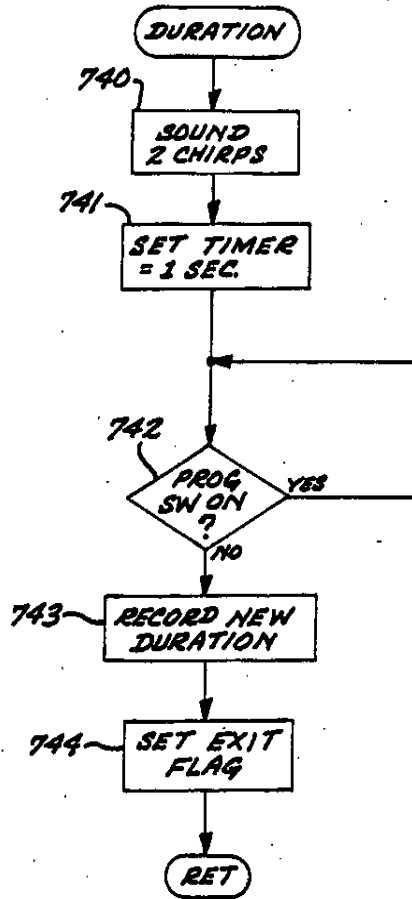


FIG. 19D

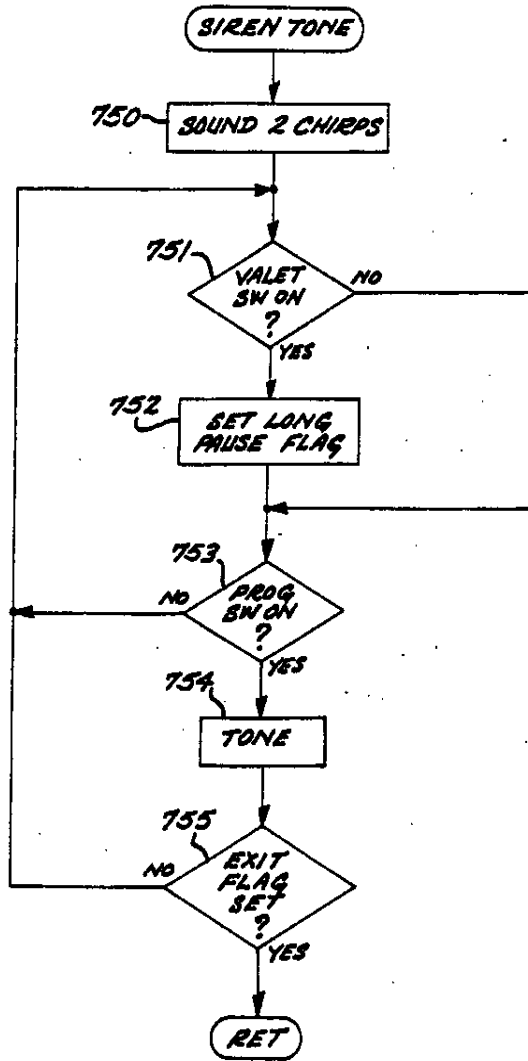


FIG. 19E

U.S. Patent

Dec. 12, 1989

Sheet 37 of 46

4,887,064

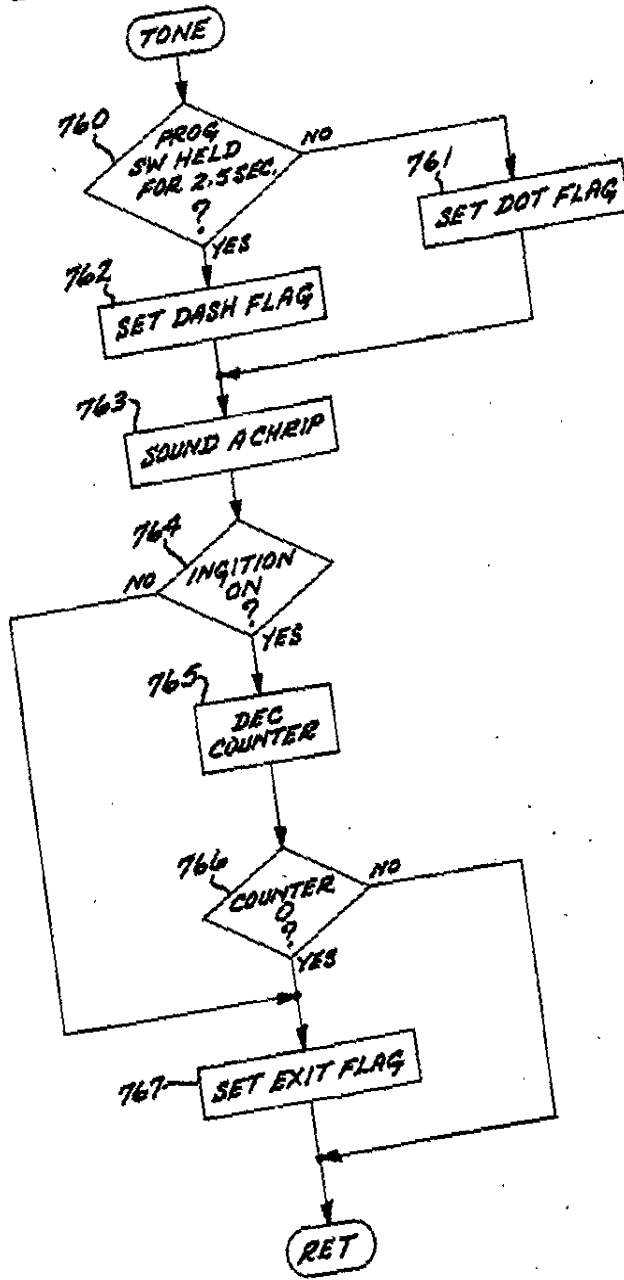


FIG. 19F

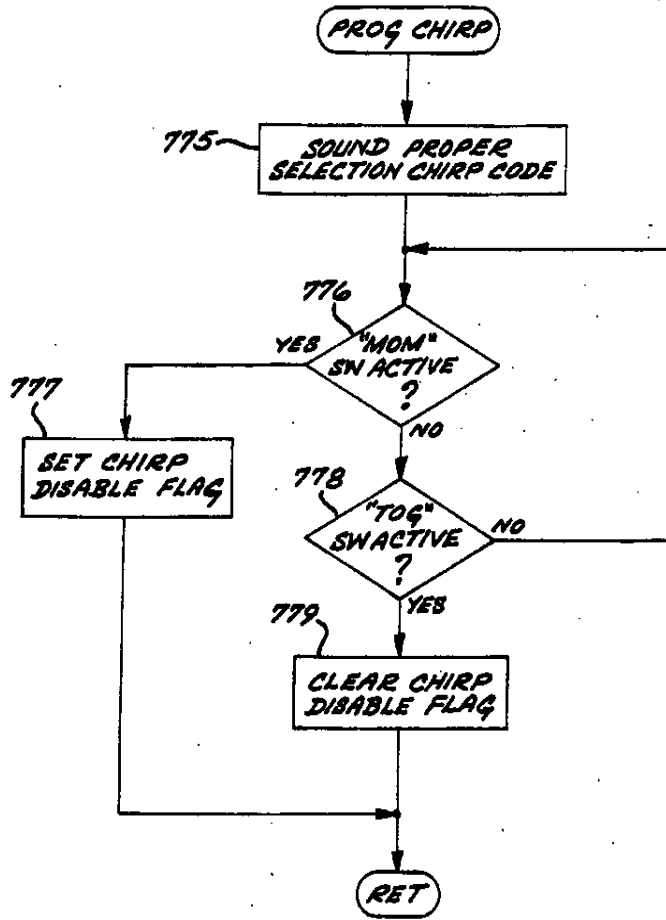


FIG.19G

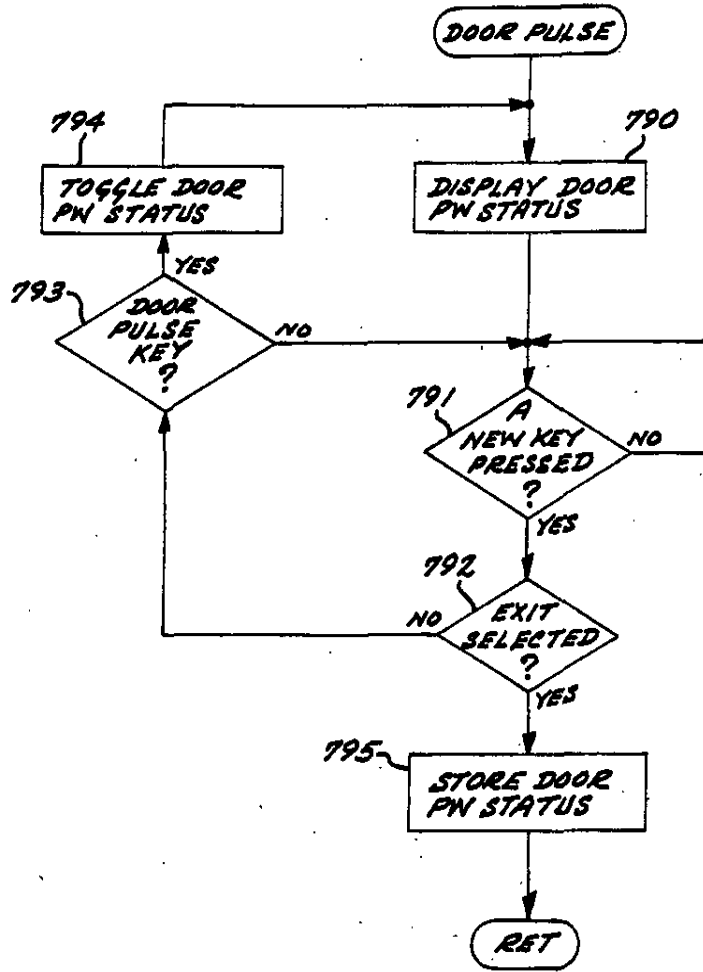


FIG. 19H

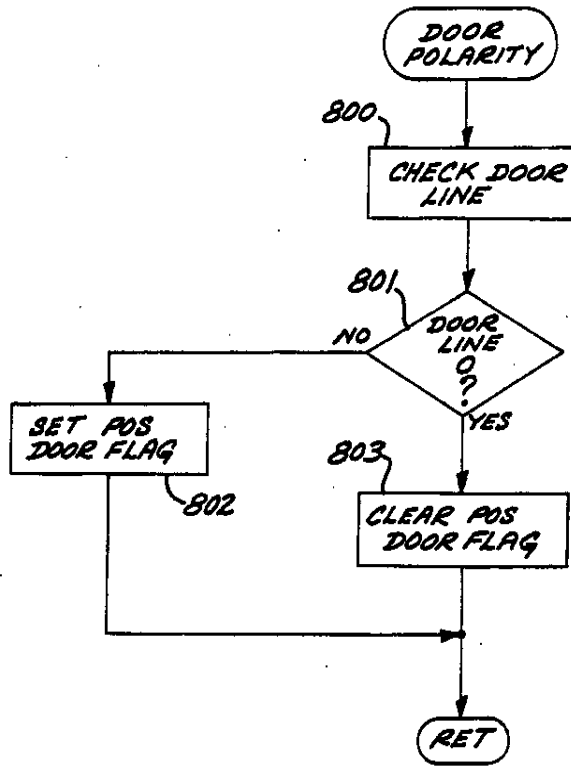


FIG. 19I

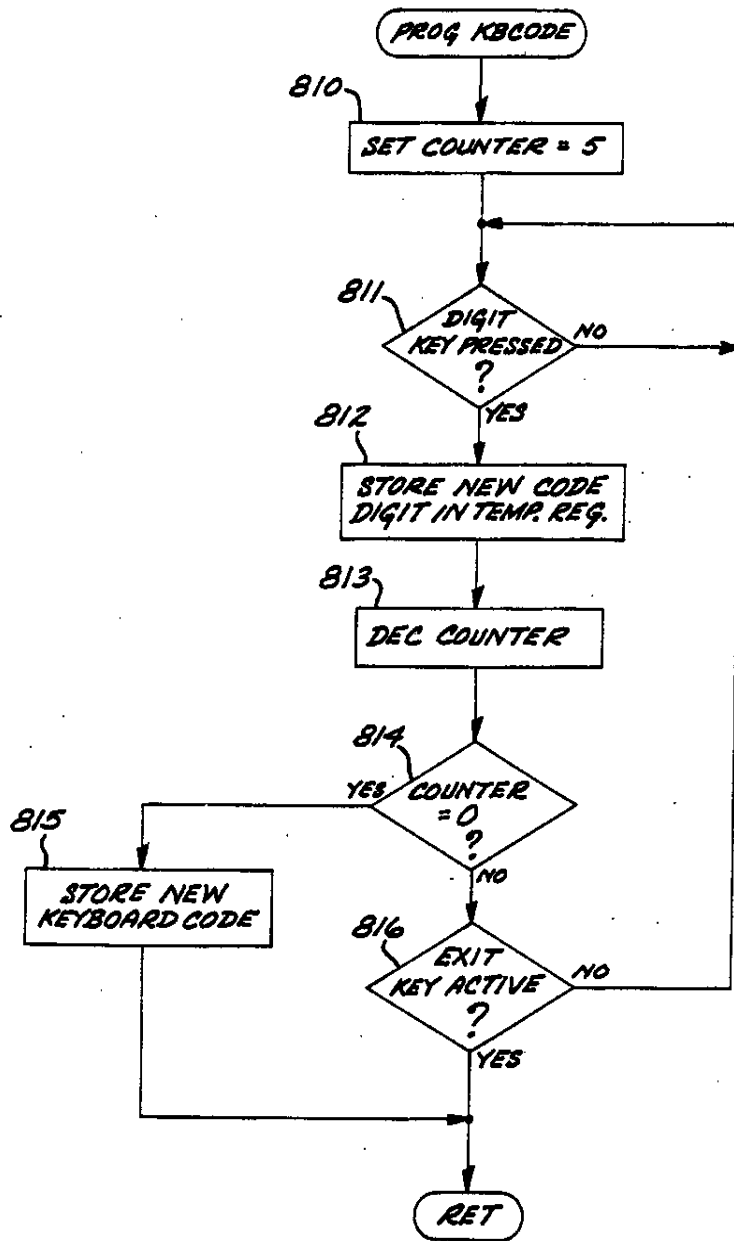


FIG. 19J

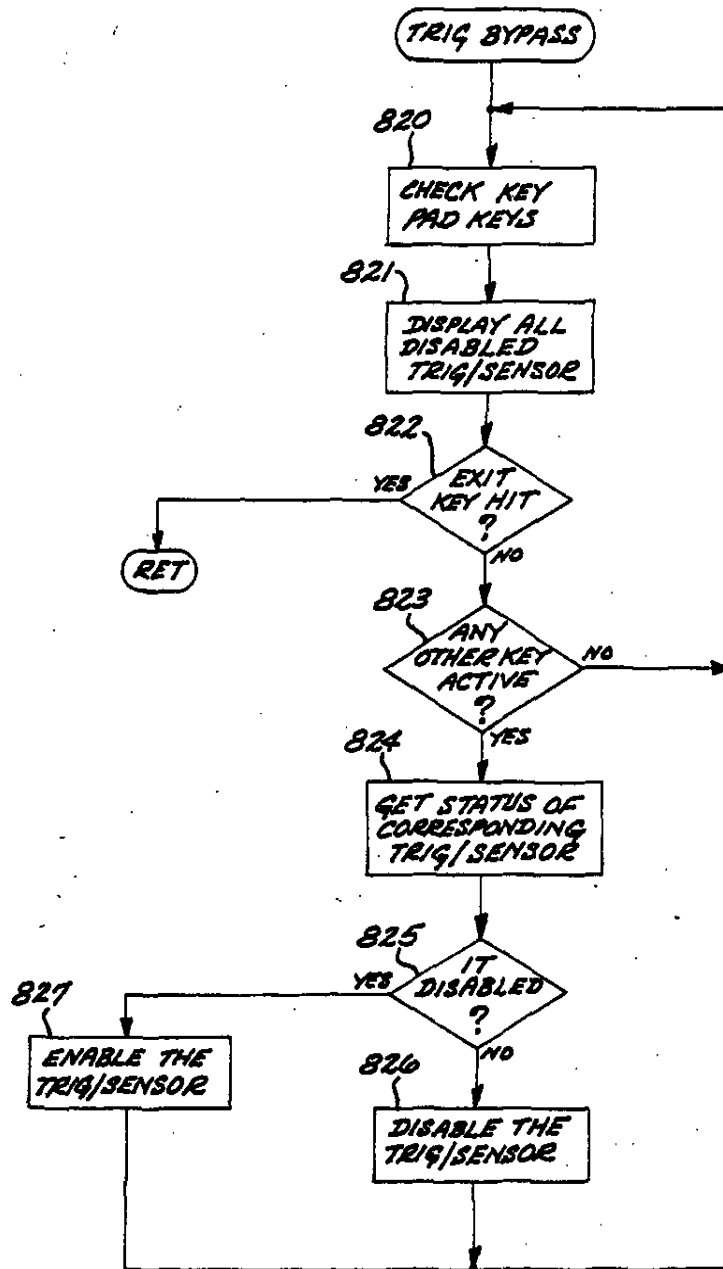


FIG. 19K

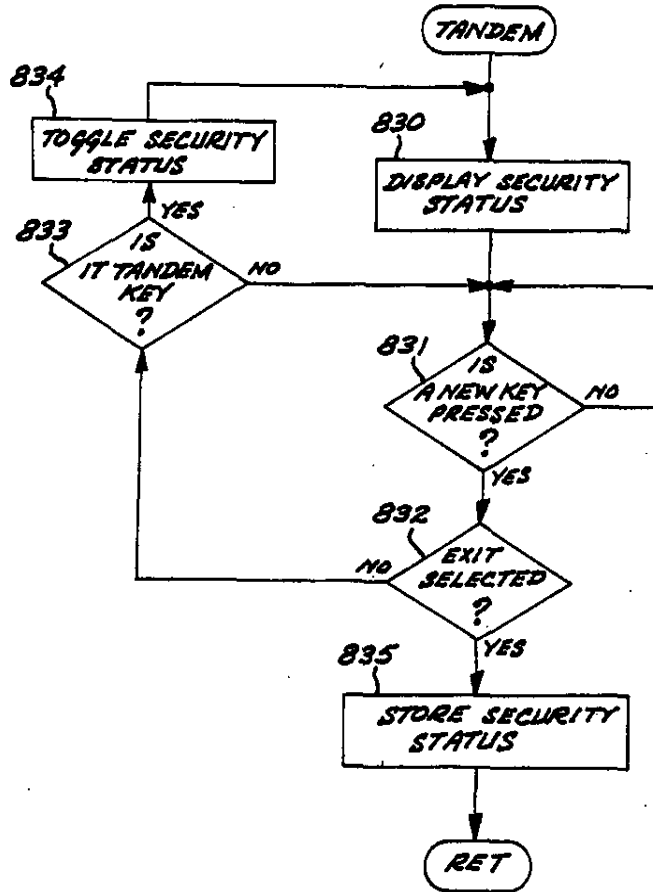


FIG. 19L

FIG. 20

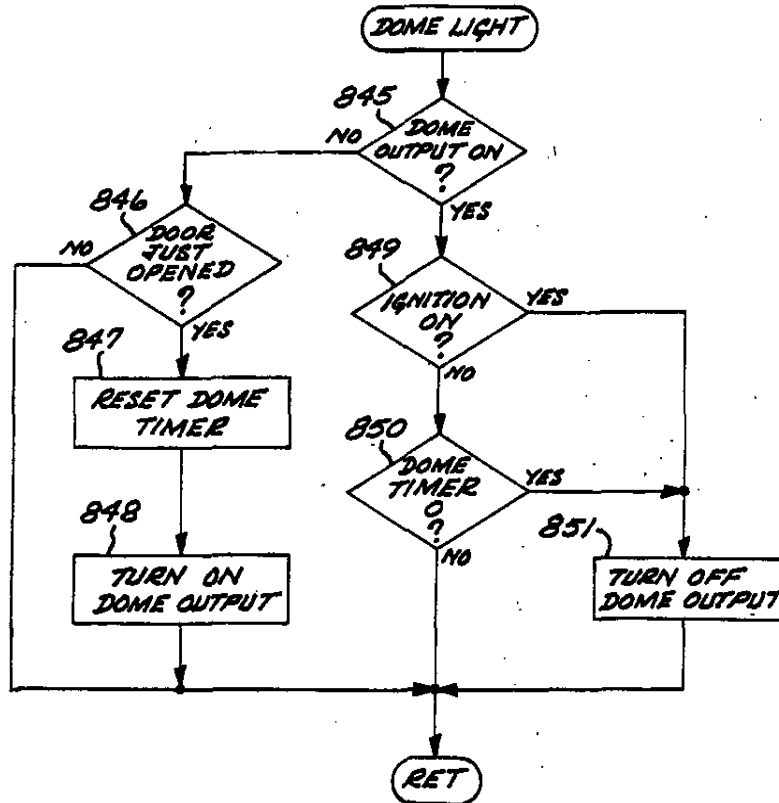
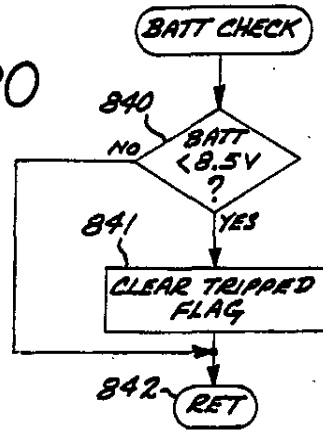


FIG. 21

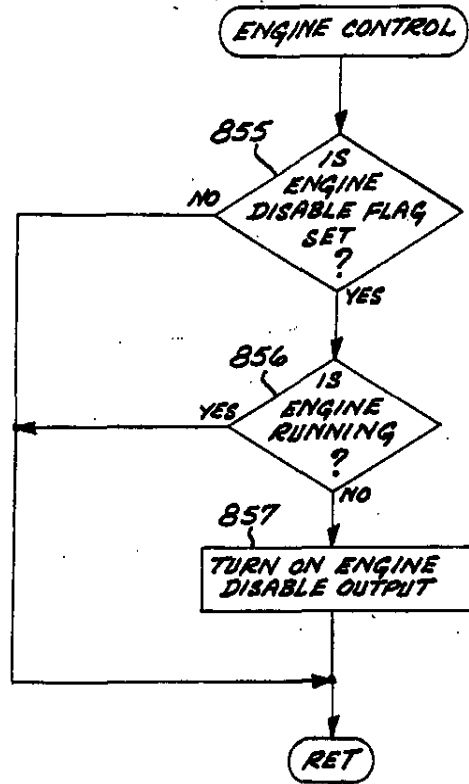


FIG. 22

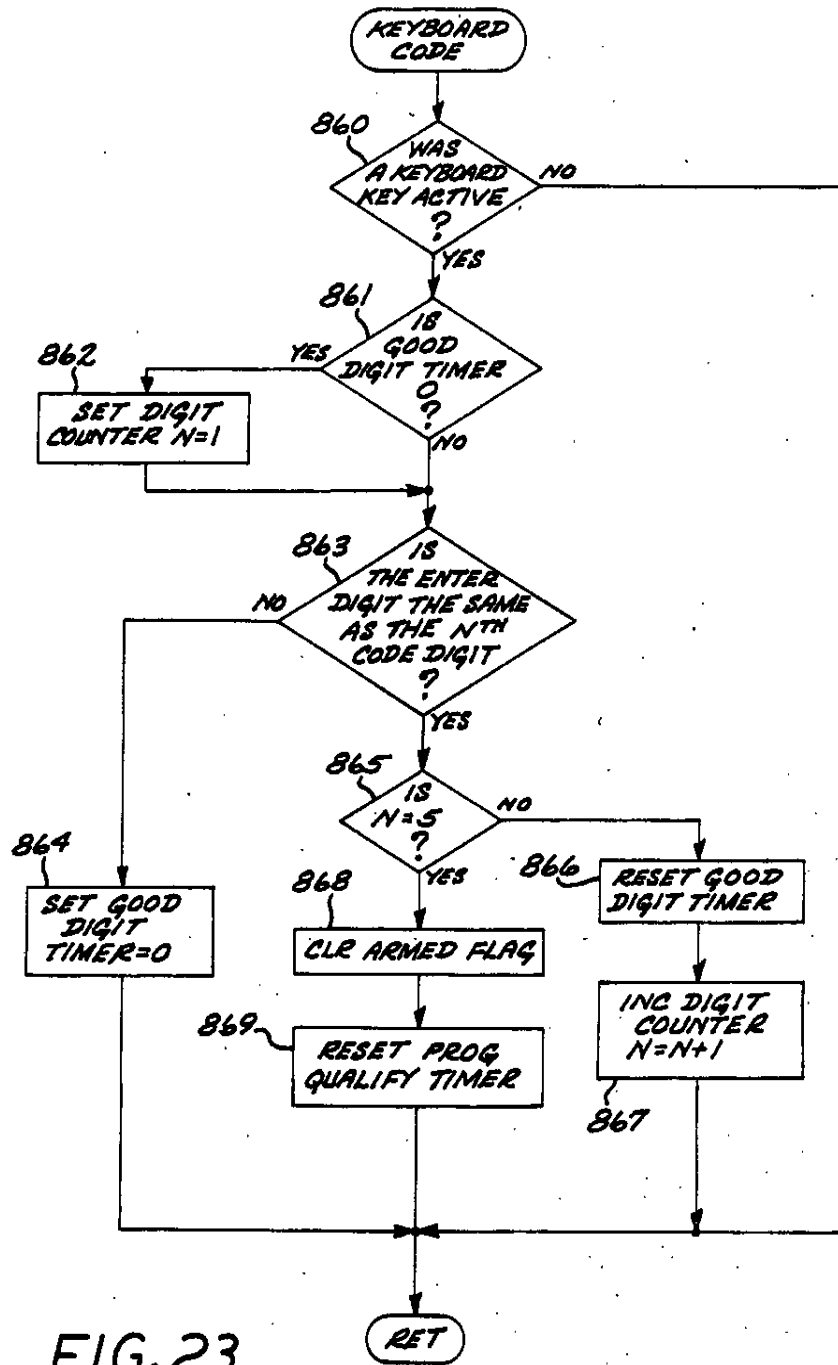


FIG. 23

4,887,064

1

MULTI-FEATURED SECURITY SYSTEM WITH SELF-DIAGNOSTIC CAPABILITY

BACKGROUND OF THE INVENTION

The present invention relates to the field of security systems for monitoring and controlling access to a secured or access restricted area, such as a vehicle of house, and more particularly to a multifunction system having the capability of self-diagnosing defective sensor and trigger devices and thereafter bypassing such defective equipment to allow the system to function.

Security systems are in wide use today to control and/or monitor access to secured or access-restricted areas. Such systems typically employ one or more sensors and/or trigger switches which are monitored or controlled by a central controller to sense intrusion or to allow controlled access. Examples of such systems include vehicle security systems and building security systems, which may be activated by either a remote switch or transmitter or by a key pad to enter a predetermined code. Entrance of the correct code typically arms or disarms the systems, opens or closes a door or the like.

The sensors and trigger typically detect attempts to intrude into the protected area, such as by way of a door or window, forcing a hood or trunk open, lifting or moving the vehicle or the like. The trigger devices may take the form of switches which are activated by the opening or closing of a door or window. The sensor may comprise a motion detector. To allow access through doors or other access point, devices which release or position locking elements, such as solenoid switches, are typically employed. Such sensors and trigger switches are prone to inevitable failure, particularly those elements positioned to monitor or control access to a heavily used door or access point. Such failure typically is manifested as an open circuit condition for a normally closed switch or sensor, or a closed circuit for a normally open switch or sensor.

Conventional security systems will not arm when a sensor indicates that a door or window is open, or when a sensor indicates that there is presently an intrusion into the protected area. As an example, a vehicle door left open will typically prevent the security system from being armed, or a window left open in a building will prevent the building security system from being armed. For the same reason, a defective sensor which indicates that a door is open irrespective of the position of the door, i.e., open or closed, will also prevent the security system from being armed. The result is that the vehicle or building owner is deprived completely of the benefit of the security system until the defective sensor is repaired.

Another disadvantage of conventional vehicle security systems is the fact that the audible alarm signals are typically generated by a horn or siren, and each particular system generates the same or similar alarm signals. Thus, when the vehicle is in a crowded parking lot or structure, and an alarm signal is generated, the vehicle's owner may not be able to determine whether it is his vehicle's system alarm or that of another vehicle. Further, many cities or other regulating authorities have enacted rules which restrict the maximum duration of vehicle alarm cycles to minimize noise pollution. However, such rules are not uniform, so that different maximum alarm cycle duration regulations are imposed in different parts of the country. The disparity in these

2

regulations creates difficulties for the manufacturers of vehicle security systems who seek to distribute their products throughout the country or in other countries.

Intruders have developed certain techniques for defeating vehicle security systems. One such technique is to disconnect and reconnect the vehicle battery, seeking to disrupt power to the security system and cause the system to be reset to the disarmed mode when power is restored.

Conventional vehicle security systems are disarmed by the use of handheld transmitter encoded with the particular authorization code, by a key or by a code entered manually via a key pad. Thus, the level of security, i.e., the actions necessary to disarm the system are typically fixed. Yet there are situations in which a lower level or security, with increased convenience in the system disarming, may be acceptable, as where the car is parked in a low risk area.

One object of the present invention is to provide a security system having diagnostic capabilities for identifying defective sensor and access control elements and bypassing such defective elements to allow the system to continue to provide some measure of protection.

Another object of the present invention is to provide a security system which upon disarming provides audible signals indicating that an intrusion was attempted while the system was armed, and to provide a visual signal when the system is disarmed to identify the intrusion point.

Yet another object of the invention is to provide a security system which allows the user to program a desired alarm siren code and or to provide an audible alarm condition whose duration may be programmed by the user, so as to provide a personalized alarm signal uniquely identifying to the user that his security system is in an alarm condition, as in the case for a vehicle parked in a crowded lot or parking structure.

Another object of the invention is to provide a security system which provides audible signals indicating the arming or disarming of the system, and which signals may be selectively disabled by the user.

Still another object of the invention is to provide a security system which provides a plurality of possible security levels, in that the user may programmably select a first disarming mode wherein the system may be disarmed simply by the use a remote handheld transmitter for transmitting a user authorization code, or a second disarming mode wherein the system is disarmed by the combination of the entry of an appropriate remote transmitter code and the subsequent manual entry of an appropriate key pad code.

Other objects of the invention include the provision of a security system which interprets the removal and restoration of system power as an unauthorized intrusion event unless a predetermined switch, such as the vehicle ignition switch, is activated when power is restored.

Still further objects of the invention are to provide a multifunction programmable security system which provides power door locking and unlocking signals to lock the doors upon system arming and to unlock the doors upon system disarming, and wherein the duration of said signals is selectively variable to adapt to door lock systems of different manufacturers; and wherein the system automatically activates the vehicle interior courtesy or dome light upon system disarming for a

4,887,064

3

predetermined time interval or until the ignition is turned on.

Other objects of the invention are to provide a multi-function vehicle security system which is programmably adaptable to trigger or sensor devices of either positive or negative polarity.

SUMMARY OF THE INVENTION

A security system is disclosed for monitoring and controlling access to a protected area, such as a vehicle. The system includes a plurality of sensor devices, each for sensing an intrusion event and providing a sensor activated signal when the event is detected. Such sensors may take the form of motion detectors, sound discriminators or switches activated by the opening or closing of a door or window, or the like.

The system further comprises means for communicating alert signals, such as for example, a siren, horn, autodialer for initiation of telephone calls or the like.

A system controller is provided to control the operation of the security system so that the system may be operated in an armed mode or in a disarmed mode. When in the armed mode the controller monitors the sensors and causes the communicating device to issue an alert signal in response to a sensor activated signal.

The system includes a self-diagnostic capability for detecting defective sensor devices and then bypassing such defective devices automatically or upon command to allow the system to be placed in the armed mode and still provide protection. In the disclosed system, the controller includes means for monitoring the states of the sensor devices, and means responsive to a system arming signal when the system is in the disarmed mode for identifying any sensor providing a sensor activated signal. The system further comprises means for bypassing the identified sensor devices, and placing the system in the armed mode wherein the state of the bypassed sensor devices does not prevent the system from being armed and the bypassed sensor devices will not cause activation of the alert communicating device.

The system further comprises means for communicating to the system user a message indicating that a sensor is defective, and further specifying the particular defective sensor. This may take the form of an audio transducer for producing a particular audio tone or tones indicative of the defective sensor condition, such as siren chirps, and an LED for generating an optical light flash sequence for identifying the defective sensor, e.g., three light flashes indicates a failed door trigger switch, or a spoken language message generated by a voice synthesizer which specifies the defective device.

The system further comprises means for warning the system user, upon receipt of a system disarm signal, of an attempted intrusion during the armed mode, and for identifying the intrusion point. The warning means may comprise a voice message generated by a voice synthesizer or an audio transducer for providing a predetermined audio sound sequence indicative of an intrusion attempt, e.g., three chirps. The identifying means may take the form of an LED for signaling by a flash code the intrusion point. This feature provides the user with a warning that an intrusion attempt has been made, which when triggered by a remote disarming signal allows the user the opportunity to take precautions prior to entering or approaching his vehicle.

The system is interactive, allowing the capability of user programmability of the particular alarm alert signal, to personalize the siren sound sequence. The advan-

4

tage of this feature is that the audio alert signal will remotely indicate to a user whether the alarm being sounded is from his vehicle, or from another vehicle, even if the vehicle is not within the owner's line of sight, as where the vehicle is parked in a crowded parking lot or parking structure.

Another feature of the invention is the means for automatically communicating an alert when the power to the system, after having been cutoff, is restored, unless the user has provided to the system a particular disarming signal, such as turning the vehicle ignition switch on prior to reconnecting power to the system. This prevents a thief from disconnecting and reconnecting power to defeat the security system.

Another feature of the invention is the provision of a user-selectable level of security, wherein the user selects whether the system may be disarmed by use of a remote transmitter alone, or in combination with a code subsequently manually entered via a keypad.

Other features of the invention include user programmability of the alarm signal duration, selective enabling or disabling of audible signals confirming the arming or disarming of the system, programmable means for providing door locking and unlocking signals of selectable duration to eliminate the need for adaptor devices for interacting with different door lock systems, selective disabling of the audible signals indicating that the system is being armed or disarmed, automatic activation of the vehicle interior courtesy light for a predetermined time interval or until the vehicle ignition is activated, and programmable sensor polarity.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features and advantages of the present invention will become more apparent from the following detailed description of exemplary embodiments thereof, as illustrated in the accompanying drawings, in which:

FIG. 1 is a simplified block diagram of a security system employing the present invention.

FIG. 2 is a schematic diagram of the receiver circuit of the security system depicted in FIG. 1.

FIG. 3 is a schematic block diagram of the controller and input and output buffers of the security system of FIG. 1.

FIG. 4 is a schematic diagram of a reset signal generating circuit, employed with the controller of FIG. 3.

FIGS. 5A and 5B are schematic diagrams of LED driver circuits employed with the controller of FIG. 3.

FIG. 6 is a circuit schematic illustrating an embodiment of the power supplies employed in the system of FIG. 1.

FIG. 7 is a schematic diagram of a receiver decoder circuit employed in an alternate embodiment of the security system of FIG. 1.

FIGS. 8A and 8B are schematic diagrams of a controller and peripheral input/output elements employed in the alternate embodiment of the security system of FIG. 1.

FIG. 9 is a schematic diagram of a key pad diode/resistor network employed with the controller of the alternate embodiment of the security system of FIG. 1.

FIG. 10 is a schematic diagram of certain output driver circuits employed with the controller illustrated in FIGS. 8A-B.

FIGS. 11-23 are flow diagrams illustrating the operation of the security system generally depicted in FIG. 1,

4,887,064

5

and more specifically with respect to the embodiments of FIGS. 2-6 and 7-10.

DETAILED DESCRIPTION OF THE DISCLOSURE

A simplified block diagram of the principal structural elements of a system embodying the invention is set forth in FIG. 1. The system includes a means for permitting the user to communicate with the system controller 70. This communicating means may take the form, in the conventional manner, of a transmitter device 55 for transmitting an encoded signal via an antenna 56. The transmitted signal is received by receiver 65 via antenna 66, and the received signal is provided in some form to the system controller 70. Additionally, or alternatively, the user communicating means may take the form of a key pad 60, which is coupled directly to the controller 70 by cable 62. The keypad 60 may comprise a plurality of digit keys 1-9, as well as additional keys or switches employed for various functions such as an "armed" switch for signaling the system to enter the armed mode. Additionally, or alternatively, the user communicating means may take the form of one or more program switches 77 manually manipulated by the user including a "valet" switch. With any one of the transmitter 55, which may be used remotely, the key pad 60, or the program switches 77, the user may input to the controller a predetermined coded message to cause the controller to initiate some action, e.g., arming or disarming the security system, sounding an alert, entering the programming mode, or the like. One type of coded message typically takes the form of a predetermined sequence of binary-valued signals, which collectively define a digital user authorization code, e.g., a predetermined N-bit word.

Power supplies 95 provide electrical power to the receiver 65 and the controller 70. In the case of a security system mounted in a vehicle, the power supplies receive the primary source of power from the vehicle battery, typically 12 volts, and convert that available power source into voltage levels required by the system, here regulated +5 volts and +8 volts.

The system triggers and sensors 75 are coupled to the system controller 70 through input buffer circuitry 80. In the case of a security system installed in a vehicle, the sensor elements may be motion sensors, door or hood position sensors, ignition switch sensors and the like. The triggers may be switches activated by a particular event such as opening or closing a door. The term "sensors" is used in a general sense in the accompanying claims to include both sensor devices and trigger devices described above.

The system 50 further employs a plurality of controlled devices, indicated generally in FIG. 1 as elements 90, which are coupled to the system controller by output buffer circuitry 85. In the case of a vehicle security system, the controlled devices may include one or more of the controlled devices 90 shown in FIG. 1, i.e., the voice synthesizer 91, siren 92, pulsed alarm 93, (hooked to parking light and/or air horns) door lock device 94, door unlock device 95, hood lock device 96, accessory 97, starter or ignition cutoff apparatus 98, LEDs 99, telephone autodialer 100, and the vehicle interior courtesy or dome light 101.

The transmitter 55 in a preferred form provides a pulse-width-modulated RF signal, wherein an RF carrier at some predetermined RF frequency is modulated by information from an internal encoder unit. As is well

6

known in the art, the transmitter may be actuated by depressing a switch, thereby generating a transmit signal encoded with information such as a multi-bit code. The specific code may be determined by the status of switches or the like comprising the encoder. The width of each pulse determines its status as a digital "1" or "0." The particular circuit arrangement comprising the transmitter 55 per se forms no part of the invention, and is not described herein in further detail. An exemplary circuit arrangement is described in the co-pending application entitled "Electronically Programmable Remote Control Access Systems" by Ze'ev Drori, Ser. No. 094,395, the contents of which are incorporated herein by this reference.

The receiver 65 is more fully illustrated in FIG. 2 and generally comprises an antenna 102 for receiving the transmitted signals, which are coupled by capacitor 106 to an NPN transistor 104 which matches the impedance of the antenna 102, and operates as a radio frequency preamplifier. A resistor-capacitor network 108 is connected to the emitter of the transistor 104. A second resistor-capacitor network 110 is connected to the base of the transistor 104.

The collector of the transistor 104 is coupled via the conductor 112 to coupling capacitor 114. An 8-volt power source from power supplies 95 is connected to the collector of the transistor 104 through a resistor 115 which isolates the transistor 104 from the power supply and from the load.

Tank circuit 118 comprises a variable inductive device 120 for adjusting the receiver regenerative frequency. A capacitor 122 couples one end of the inductive device 120 to the conductor 112. The same end of the inductive device 120 is also coupled through capacitor 124 to a variable resistor 126, also connected to the 8-volt power source.

The conductor 112 is also connected to a local oscillator 128 which includes a transistor 130 having a capacitor 132 connected across its collector and emitter. The base of the transistor 130 is connected to the voltage source through the resistor 126. The emitter of the transistor 130 is connected to inductor 134. This arrangement of the local oscillator including the transistor 130, the capacitor 132 and the inductor 134 is designed to detect the pulses included in the received signal.

The inductor 134 is connected to conductor 136 which carries the detected signal. The detected signal pulses are passed through a resistor 138 and a capacitor 140 and to a signal amplifier 142 in the form of an NPN transistor. Another resistor 144 is connected across the collector and the base of the transistor 142, whose emitter is grounded and is also connected to a coupling capacitor 146.

The collector of the transistor 130 is connected to a pair of load resistors 148 and 150. The 8-volt power supply is connected through a load resistor 152 to the collector of the transistor 142. The reference voltage applied to the comparator 154 is developed by the voltage divider circuit comprising resistors 156 and 157. The comparator 154 receives a signal for comparison from the collector of the transistor 142 through a coupling capacitor 158. When the inputs to the comparator 154 compare, an output is generated and inverted by an inverter 160.

The output of the inverter 160 is then introduced into the controller 70, as is more fully illustrated in FIG. 3. In this case, the output from the receiver 65 is introduced into an exclusive OR gate 162 (acting as a pro-

4,887,064

7

grammable inverter) which has an output to the controller 70. The controller 70 comprises a microcomputer, with some internal RAM and nonvolatile memory capacity, such as the NEC 80C49H microcomputer.

The plurality of sensors and triggers 75 (FIG. 1) are coupled to the controller 70 by a buffer circuit 80 comprising the diode network 212 shown in FIG. 3. The trigger and sensor 75 are connected to nodes 201-210 which connect to the network 212 and to node 210. By way of example only, a positive trigger device may be connected to node 201, first and second sensor devices to nodes 202 and 203, a negative trigger at node 204, an "immediate" trigger device at node 205, a hood position sensor at node 206, an automatic arming disable switch at node 207, program switches 77 (the "valet" and "hood" switches) at nodes 208 and 209, a normally closed trigger at node 210, and an ignition switch "on" or "off" sensor at node 211. The pins P1-P8 are monitored by the microcomputer 70, enabling the microcomputer to monitor the states of the trigger and sensor devices, thereby monitoring the protected areas of the vehicle.

The particular triggers, sensors and switches are described by way of example for a vehicle security system implementation. Positive and negative triggers are provided so that the system may be employed with either a positive or negative polarity door trigger switch. The "immediate" trigger device is typically connected to the vehicle trunk or back door, for generating an immediate alarm when the trigger is activated. The hood position sensor provides a signal indicative of the position of the hood, i.e., closed or not closed. The normally closed trigger coupled to node 270 is a trigger device that is normally grounded, and is activated when the trigger is no longer grounded. Such a trigger is normally connected to the vehicle radio, to signal when the radio has been removed.

Significantly, the sensors and triggers 75 and program switches 77 are coupled to the controller 70 in such a way as to allow the controller to monitor the individual status of each device. This is an important element in implementing the self-diagnostic feature of the invention.

Pin P10 of the microcomputer 70 is also monitored to receive information from the receive 65.

Pins P11-P20 of the microcomputer 70 are employed as output pins to control the various controlled devices 90 employed with the system. The output buffer circuitry 85 comprises hex driver device 214, for example, a type 76C906 device, and pullup resistor network 216 connected to output lines 218-223, which are in turn connected to a corresponding plurality of power CMOS transistor devices, one of which is indicated as device 226. The output of the power transistor 226 is diode-coupled to a 12 v power source and is connected to a controlled device at node 230. Thus, the driver circuit 214, network 216, power transistor 226 and diode connection to the power source serves as part of the output buffer circuit 85 to enable the low level microcomputer output signals to drive a controlled device such as, for example, a siren, pulsed alarm, door lock, door unlock, a hood lock, and the like which require substantial power to operate, e.g., by actuating relays. Nodes 231-235 are connected to similar power transistor devices, which for the sake of clarity are not shown. These nodes are also used to control various controlled devices.

8

For this example of the invention, line 218 controls the siren device 92, line 219 the pulsed alarm 93, line 220 the door lock device 94, line 221 the door unlock device 95, line 222 the hood lock device 96 and line 223 an accessory device 97, the dome light 101, or the autodialer 100.

Another output pin P20 of microcomputer 70 is coupled to an inverter circuit 238 whose output is connected to driver transistor 240. The collector of transistor 240 drives power transistors 242 and 244 to provide additional control nodes 248-250 to control various controlled devices, such as the starter/ignition cutoff device 98, accessory 97 and the like.

Output pins P17-P19 are connected respectively to the circuit shown in FIG. 4 and the LED driver circuits of FIGS. 5A and 5B.

An oscillator circuit 252 provides a stable oscillator frequency signal to the microcomputer for use as the device clock. The microcomputer 70 receives +5 volt power from battery circuit 254 and from power supplies 95.

The microcomputer 70 receives a reset signal on pin P21 from a reset signal generating circuit shown in FIG. 4. The reset signal generating circuit comprises a retriggerable one-shot CD4538 device 260 triggered by pin P17 of the microcomputer 70, which periodically (e.g., every 10 milliseconds) provides a pulse to one-shot device 260. The \bar{Q} output of device 260 serves as the trigger to one-shot CD4538 device 262, whose Q output drives transistor 264. The collector of transistor 264 is coupled to ground through capacitor 266, with the reset signal being developed across the capacitor 266. In the event that the periodic pulses from the controller pin P17 are interrupted, the Q output of device 262 will go "high," turning on transistor 264 and generating a reset pulse. The signal "E" coupled to the base of transistor 268 is generated by the voltage supply 95, as will be described with respect to FIG. 6. The signal "E" goes active in the event the regulated 5-volt supply is not available from the supply 95, indicating that the vehicle power has been removed, or the vehicle battery voltage has been drained. The emitter of transistor 268 is coupled to the base of transistor 270, to provide a means for generating a reset pulse when the 5-volt supply (95) is no longer available.

Thus, the reset or "watchdog" circuit of FIG. 4 will generate a reset pulse when the controller pulses (pin P17) are no longer provided, or when power is removed or impaired.

FIGS. 5A and 5B illustrate respective driver circuits for the green and red LED devices 99 which are employed in the disclosed embodiment to provide a means for visually communicating with the user of the system. Pin P18 of the microcomputer 70 controls the green LED driver circuit of FIG. 5A and pin P19 controls the red LED driver of FIG. 5B. The green LED driver circuit comprises an inverter device 272, NPN transistor 274, PNP transistors 276 and 278 connected in the manner shown in FIG. 5A. The operation of the driver circuit of FIG. 5A as well as that of FIG. 5B will be readily understood by those skilled in the art. In the case of the security system installed in a vehicle, the LEDs 99 may be mounted on the vehicle instrument panel or dashboard.

Referring now to FIG. 6, the circuitry for the power supplies 95 is shown. The circuitry develops regulated 5 and 8 volt sources, employing a pair of type LP2951 regulator devices 280 and 282. Nodes P1 and P2 are

connected to the positive and negative terminals of the vehicle 12-volt battery, respectively. The positive terminal is a diode coupled to pin 8 of each of the regulator devices 280 and 282. As will be apparent to those skilled in the art, regulator device 280 is appropriately configured to provide a regulated +5 volt supply level at node 288, and device 282 is appropriately configured to provide a regulated +8 volt supply level at node 290. The devices 280 and 282 each provide error outputs at respective nodes "E" and "H," which are active when the +5 volt or +8 volt supply is not available, within some predetermined margin, e.g., $\pm 5\%$ of +5 volts or +8 volts. Node H, the error signal for the regulator 282 for the +8 volt supply, is coupled to pin P23 of the controller 70. By monitoring the state of the regulator error signal at pin P23, the controller determines when the +8 volt supply is no longer available. In such case, the controller will disable operation, as will be described more fully hereinafter with respect to the "battery check" function of the system.

In the embodiment of the receiver and controller set forth in FIGS. 2-6, the user's authorization code is entered via a remote transmitter 55. In an alternate embodiment, the user's authorization code may also be entered manually by the user via a key pad 60, which in the case of an automobile security system is typically mounted inside the vehicle in a location accessible to the vehicle driver. Thus, the system may comprise a remote transmitter 56 and a receiver 65, but also comprises the key pad 60 for allowing code and other information to be entered manually by the user into the controller 70. Such an alternate embodiment is illustrated in FIGS. 7-10.

The receiver employed with the alternate system may be identical to the receiver described with respect to FIG. 2, but may further comprise an external decoder circuit for comparing the received signal with the stored authorized code to determine whether the received signal matches the stored code. Thus, in FIG. 7, the received data from the receiver (FIG. 2) is provided to the type MC14502A device 302 which acts as a decoder, comparing the received data bits with the stored data bits defined at pins CD1-CD9 by the connections made between the node network 304. The connections are typically all made on the circuit board, and then personalized to provide a unique user code by scratching away the appropriate traces. If the input data bit sequence matches the stored code sequence, then node VT of the correlator device 302 is activated, turning on buffer transistor 300, whose collector output is in turn coupled to the microcomputer 304 (FIGS. 8A and 8B) which comprises the controller in this embodiment.

Referring now to FIGS. 8A and 8B, the controller and buffer circuitry for the alternate embodiment is disclosed. Here, a plurality of peripheral devices are arranged in a common bus arrangement to communicate with the microcomputer 304. Each of devices 310, 312, 314, 316, 318 and 320 are type 74HC373 devices having eight pins coupled to the 8-bit data bus 306 which is in turn connected to pins P1-P8 of the microcomputer 304. The output disable pin OD of device 310 is controlled by pin P9 of the microcomputer 304, the OD pin of the device 312 is controlled by pin P10, and the OD pin of the device 314 is controlled by pin P22. Similarly, the latch enable pins LE of devices 316, 318 and 320 are controlled respectively by pins P17, P18 and P22 of the microcomputer 304. Thus, only one of the six peripheral devices will be enabled by the mi-

crocomputer at any given time, so that the input/output pins P1-P8 of the microcomputer will be receiving data from one of devices 310, 312, or 314, or writing data to one of the devices 316, 318 or 320 via the data bus 306 at any given time.

The data input D1 of device 310 is coupled to the digit 9 signal associated with the key pad 60. Pin D2 is coupled to the "armed" switch on the keypad 60. Data input pins D3-D6 are pulled up to 5 volts. Pin D7 is coupled to the sensor "2" of the system. Pin D8 of device 310 is coupled to the hood sensor of the system. Thus, the states of these various switches and sensors may be read by the microcomputer by enabling the outputs of the device 310.

The data input pins D1-D8 of device 312 are coupled to the digit 1-8 signals associated with the key pad 60.

Six selected ones of the digit 1-9 signals are coupled to the data input pins D1-D6 of device 314 by wire wrap connection network 322. This allows a unique user code to be hardwired into the controller at the factory in dependence on the particular ones and sequence of the selected digits of the key pad.

The output from the external decoder (FIG. 7) is coupled to pin P23 of the microcomputer. The ignition sensor is coupled to pin P24.

A plurality of other sensors, switches and triggers are coupled to pins P11-16 of the microcomputer 304, including the ignition sensor, sensor 1, the "immediate" trigger, the negative trigger, the key pad program or "valet" switch and the key pad automatic alarm switch. The microcomputer 304 reads the states of these devices by interrogating pins P11-16.

As with the embodiment of FIGS. 2-6, the controller 304 is coupled to the sensors and triggers in such a way as to individually determine the status of the sensors and triggers, to implement the self-diagnostic feature as will be described in more detail hereinafter.

The data on the 8-bit data bus 306 will be latched into the output pin latches of device 316 when the latch enable pin of the device is activated by the microcomputer. This provides the control signals for controlling certain of the controlled devices, including a pulsed alarm, hood release, pager control, ignition cutoff, door lock, door unlock and piezoelectric (buzzer) control. These control signals are coupled to a driver circuit (FIG. 9) to develop the appropriate voltage signals for controlling relays or driving the particular controlled element.

The data on the 8-bit data bus 306 will be latched into the output pin latches of device 318 when the latch enable pin of the device is activated by the microcomputer. This provides the control signals at pins Q1-Q3 which are converted by the hex driver device 324 into drive signals for driving the various key pad LEDs as illustrated in FIG. 8B. (In this embodiment, each digit key of the key pad has associated therewith a corresponding LED.) Pin 20 is also coupled to the hex driver device 324 to provide the drive signal for activating the "arm" switch or key LED on the key pad. The Q1 output of device 320 is also coupled to the driver device 324 to provide the drive signal for the LED 1 on the key pad. Pin P19 of the microcomputer is coupled through an inverter chain to the hex driver device 324 to provide the signal controlling the system siren.

The data on the 8-bit data bus 306 will be latched into the output pin latches of device 320 when the latch enable pin of the device is activated by the microcomputer. This provides the control signals at pins Q1-Q8.

4,887,064

11

The signals at pins Q2-Q8 are coupled to the hex driver device 326 to provide the drive signals for the key pad LEDs 2-8.

Referring now to FIG. 9, a resistor-diode network is illustrated for converting the states of the key pad keys into usable signals for interrogation by the microcomputer 304. The network provides two sets of "digit" signals, one set for connection to device 312 and the other set for connection to the wirewrap network 322 (FIG. 8A).

FIG. 10 illustrates the circuits which convert the control signals for controlling the controlled devices comprising the accessory, pulsed alarm, hood release, ignition cutoff, door lock and unlock, and the like, into drive signals for operating these devices or relays associated therewith. Only exemplary ones of the circuits are illustrated, since the circuits are identical. For example, the circuit for providing the accessory drive signal comprises transistors 330 and 332 which cooperate to provide selectively a 12-volt drive signal.

The security system of the invention comprises a number of significant features and functions. One feature of the invention is a self-diagnostic capability for detecting defective sensors and trigger devices and thereafter disabling the defective sensor or trigger to allow the system to be armed. In the embodiment shown in FIGS. 2-6, any defective system sensor or trigger is found and automatically disabled each time the system is armed. Moreover, an audible notification is provided that a defective device has been located, and the particular defective device is identified by an LED flash code and or by an audible message generated by a voice synthesizer. In the embodiment of FIGS. 7-10, the system automatically locates and identifies any defective sensor each time the use seeks to arm the system. The system user may then manually and selectively bypass any identified defective sensor or trigger using the key pad if he does not wish to immediately service the defective device. Thus, in contrast to many conventional systems which can not even be armed if there is a defective sensor or trigger device, the present system automatically detects and identifies any defective sensor or trigger, and thereafter either automatically or user-selectively disables such devices to allow the system to be armed. Therefore, some security protection is still available, even though at some reduced level due to the disabled sensor or trigger.

Another feature of the present security system is that, upon disarming the system, a visual and audible indication is made to the system user if any intrusion has been detected while the system was in the preceding armed state. This is accomplished in the present embodiments by causing a first predetermined audio sound pattern (e.g., two chirps) to be generated if no intrusion was detected, and a second particular audio sound pattern (e.g., four chirps) to be generated if an intrusion was generated. In the case wherein the user has disarmed the system via the remote transmitter, this is an added safety feature by warning the user of the intrusion before he nears the vehicle. The point of intrusion is also identified by a visual signal, e.g., a particular LED flashcode corresponding to the tripped sensor or trigger device, or by a voice synthesized signal providing a speech message identifying the intrusion point (e.g., "the driver's door was opened").

Another novel feature of the present system is the user programmability of a personalized siren code. This allows a system owner to remotely determine whether a

12

particular alarm signal being generated is from his system. Thus, if a system is employed as a vehicle security system for a vehicle parked in a crowded lot or parking structure, the owner can determine whether his vehicle has been tampered with simply by listening for his personal siren code. In these embodiments, siren codes in the form of short "dots" and long "dashes" are employed. Further, the user may programmably determine the duration of each alarm cycle, to thereby comply with local ordinance.

The system also includes means for detecting the disconnection or disabling of power to the system and automatically generating alarm signals when power is restored unless a switch (e.g., the ignition switch) has been set by the user. This prevents the system from being defeated by a thief through the technique of disconnecting and thereafter reconnecting the vehicle battery.

The system may be programmed to directly provide door locking and unlocking signal pulses of the correct duration for the particular vehicle. At present, depending on the vehicle manufacturer, either one or three second pulse durations are required. The installer of the system programs the controller to provide door lock and unlock control signals of the appropriate duration for the particular vehicle. This feature eliminates the need for the use of interface devices for driving the door locking systems, as has heretofore been required.

The system has two security modes, and the user may programmably select the desired security mode, depending on the security level desired. In one mode, with a lower security level, the system may be disarmed using only the remote transmitter to enter the user authorization code. In the second mode, with a higher security level, to disarm the system requires the use of the remote transmitter to enter the appropriate transmitter code and the subsequent entry of the appropriate authorization code via the system keypad. This allows the user to select the level of security provided by the system. Thus, when the vehicle is to be left in a low-risk area, the user may opt for the lower level of security, to gain the convenience of not having to enter manually the keyboard code to disarm the system.

Another safety and convenience feature of the security system is that the vehicle interior courtesy or dome light is automatically activated when the system is disarmed by the remote transmitter for a predetermined time interval or until the ignition switch is turned on. The system may be programmed to operated with sensors and triggers of either negative or positive polarity.

To further explain the operation of the invention, a general flow diagram of the operation of the system is set forth in FIG. 11. As will be apparent to those skilled in the art, the desired operation of the system is achieved by appropriate programming of the controller 70 (or 304) to execute instructions achieving the functions indicated in the flow diagram.

The operation commences at step 400 on system powerup with the RESET function. This results in the reset circuit (FIG. 4) providing a reset signal to the controller to initialize the various parameters and flags utilized in the microcomputer. The reset function also provides a unique function, detecting whether power has been disconnected from the security system and then reconnected. The system will activate the alarm if the reconnection of power is unauthorized. The purpose of this feature is to prevent a thief from disconnecting power to the vehicle and therefore the security

system by disconnecting the vehicle battery, and then reconnecting the power to defeat the security system since the system would otherwise be powered up in the unarmed mode, allowing the thief to enter the vehicle without activating the alarm. The "reset" feature of the system is more fully described with respect to FIG. 12.

The next function performed by the system is the "CHECK RECEIVER" function 402. This step is performed for the alternate embodiment of FIGS. 7-10, which employs an external decoder to determine whether the received message matches the predetermined code sequence. The microcomputer interrogates pin P23 of microcomputer 304 to determine whether the decoder (FIG. 7) has detected receipt of the appropriate code. This step is not employed by the embodiment of FIGS. 2-6, since the decoding operation in that embodiment is internal to the microcomputer 70.

The next step 404 in the general operational flow is to decode the received RF signal, in the case of the embodiment of FIGS. 2-6, wherein decoding internal to the microcomputer 70 is employed. This function is a correlation of the received sequence of digital data bits with the stored authorization code. If the received signal matches the stored code, then a flag is set indicative of the condition of a correctly entered user authorization code. The decode function for the internal decoder is interrupt driven, with assembly of the incoming data bits occurring in the background until a "dead period" is detected with no data coming in for a predetermined period of time. Then the received bit sequence is compared with the stored data, and flags are set accordingly. The internal decoding function is described more fully with respect to FIGS. 13A-C.

The next function to be performed is the ALARM mode function 406. Here, the alarm mode is commenced, if appropriate, as determined by the appropriate software flags, i.e., the "TRIP" or "PANIC" flags. Thus, if the alarm mode has been triggered, then controlled devices such as the siren, the dome and parking lights and the like as programmed to occur during an alarm event are activated. The alarm mode starts a timer for the alarm duration. If either the "PANIC" or "TRIP" flag is cleared during the timeout, the alarm mode ends immediately. Otherwise the flags are cleared at the end of the alarm interval. The alarm mode is described more fully with respect to FIG. 14.

The next function in the overall sequence is the VALET MODE function 408. During this mode the controller determines if the system is disarmed, and if disarmed, checks the ignition switch. The mode output is a VALET flag. The valet mode is entered by turning the ignition on and toggling the program "valet" switch. This sequence of events disables the alarm system. To exit the VALET mode, the vehicle ignition switch is turned on and the program "valet" switch is toggled to the off position. The valet mode allows the security system to be disabled so that the vehicles may be left in the care of an authorized person, such as a valet, service technician or the like. Thus, if the valet mode is properly entered, the VALET flag will be activated.

The next function 410 to be accomplished by the system is to check the triggers and sensors of the system. For the embodiment of FIGS. 2-6 this is accomplished by reading the states of the microcomputer 70 pins P1-P9. In the embodiment of FIGS. 7-10, this is accomplished by respectively activating the outputs of devices 310, 312 and 314, and by reading the states of

the data pins P1-P8, and by reading pins P11-P16. For each active line or device, a flag is set. The flag will be cleared when the particular line or device is no longer active.

The next function in the main loop (FIG. 11) is the CONTROL function 412. This is described in detail with respect to FIGS. 15A-15C. In general, the control function responds to the decoder outputs. When the command is received to arm the system, the controller checks the sensor and trigger flags. If no sensor or trigger line is active, i.e., none of the device flags are set, then the controller enables two "chirps" (a chirp is sounded by a pulse applied to the siren 92) and then sets the ARMED flag. If there is an active trigger or sensor, four chirps are sounded and the controller provides information to an LED register comprising the controller 70, indicating which sensor is active, i.e., setting a flag which will be used to communicate visually to the user which sensor is defective. If the decoder signal is to disarm the system, then the controller sounds one chirp if there was no tampering with the controlled area. If tampering occurred during the time the system was armed, the chirp counter is set to 3 (step 563, FIG. 15B), the controller 70 provides the LED register with information as to which sensor or trigger was tampered with (step 564). During this function, the controller also recognizes whether the system is in the "panic" mode, which is set by a two and one-half second transmitted signal from the user transmitter, and sets the PANIC flag in this event. If during the panic mode the operator transmits the correct authorization code, then the controller terminates the panic mode. Otherwise the panic mode continues until the alarm timer runs out. During this function the controller also set the duration for the door unlock/lock control signal.

Once the CONTROL function has been completed, then at step 414, the decision is made as to whether the system is armed, by checking the ARMED flag. If the system is armed, then the next function is the armed mode function 418. If the system is not armed, the disarmed mode function 416 is performed.

A timer is initiated in the ARM mode (FIG. 15D) to disable the sensor "two" (e.g., a motion or shock detector or sound discriminator) line (coupled to pin P2 of the controller 70 in FIG. 3) for five seconds. After the initial five seconds, both trigger and sensor lines are enabled. A counter function is provided for counting how many times each sensor or trigger is activated consecutively. After ten consecutive alarms by a particular sensor or trigger, that device will be disabled. This prevents noise pollution and battery drain caused by what would otherwise be a continuing alarm signal. If a sensor or trigger is active, a TRIP flag is set and information is placed in a register which identifies the particular trigger or sensor which tripped the alarm. The LED control mode 420 responds to this data when the system is disarmed. The siren sound is activated here also so that the siren responds to the personalized siren bit pattern, as will be described below with respect to FIG. 19E, and sets the siren flag accordingly.

The DISARMED function 416 controls the passive arming of the system. This is described in further detail with respect to FIG. 15B.

The LED control function 420, when the system is armed, sets the red LED flag to flash with the appropriate message as indicated by the data stored in the LED register. If the system is disarmed, the green LED flag will be set to flash in the appropriate sequence. If the

15

valet mode has been entered the green LED flag will be set. The LED control is described in further detail with respect to FIGS. 18A-C.

The next function in the general operation flow is the OUTPUT CONTROL function 422. Here the controller examines the flag for each output line of the controller 70 for a controlled device, and if set, will turn that output line on. If the flag for a particular output line is cleared, the controller will turn that line off. Thus, this function activates and deactivates the controlled devices 90, in dependence on the state of the software flag associated with the particular device.

The next function is the CHECK SWITCHES function 424. During this step, the controller checks the status of all switches other than sensors and triggers, i.e., the ignition switch, the program ("valet" and hood) switches 77, and the passive arming disable line. The controller sets flags as appropriate for each line.

The next function is the ENTER PROGRAM function 426. The purpose of this mode is to program information into the system, e.g., setting the duration of the alarm cycle (from 1 to 255 seconds), the pattern of the siren, as well as the other programmable features described more fully with respect to FIGS. 19A-L. For the embodiment of FIGS. 2-6, this mode is entered when the ignition switch is on and the program "valet" switch is toggled on and off within one second. The system chirps once to signify that the program mode has been entered and the green LED is turned on. The programming mode can be aborted by turning the ignition switch off.

The CHECK BATTERY function (step 430), shown in FIG. 20 operates to detect the condition wherein +5 volts is not available to the security system, and disables the system in that event to avoid further draining the vehicle battery.

The DOME LIGHT function 432 allows the user to have the interior courtesy or dome light activated for a predetermined interval after the system is disarmed. This function is described in more detail with respect to FIG. 21.

Another function performed during the main loop is the "ENGINE CONTROL" function 434. As will be described hereinbelow with respect to FIG. 22, this function selectively disables the vehicle engine to prevent unauthorized operation of the vehicle.

The KEYBOARD CODE function (step 436) allows the user to enter an authorization code manually via the key pad 60. This function is discussed in further detail with respect to FIG. 23.

After step 436 has been performed, the operation flow loops back to step 402 to commence the loop again. The entire main loop takes only a short period of time to complete, on the order of milliseconds.

Selected ones of the particular functional modules described above will now be described in further detail. FIG. 12 shows the RESET module which is activated when the +5 volt power supply to the system 50 is interrupted and restored. Upon power up, the controller 70 input/output lines are initiated at step 450. At step 452, the registers of the random access memory of the controller are initialized. At step 454, the ignition switch state is read and if turned on, the ARM flag is cleared at step 456, and the program operation returns to step 402 of the main operation loop. If the ignition switch is not turned on, the ARM and TRIP flags are set, since this is interpreted as an unauthorized power up

4,887,064

16

of the system, and program operation returns to step 402.

The internal DECODE module 404 is illustrated in further detail with respect to FIGS. 13A-B. FIG. 13A shows the bit assembly operation carried out by the controller 70 as data is being received by the receiver. This background operation is continuously performed, even as the operational flow is at various functions within the main loop of FIG. 11. The receipt of a bit (rising edge) from the receiver at pin P10 of controller 70 results in a hardware interrupt, which shifts operation to the bit assembler (FIG. 13A). At step 462, if a rising edge of a received pulse is detected, then at step 464 a "bit width" timer is started, the bit count for the particular received sequence of bits is incremented (step 466), and at step 470 operation returns to whatever step in the main loop in which the interrupt occurred. If at step 462, the rising edge of a pulse is not detected, then at step 472 the present pulse width is determined, and if not within the predetermined limits (step 474), then at step 476 an ERROR flag is set. At step 470 operation returns to the main loop step at which the interrupt occurred. If the pulse width is within limits, then at steps 478, 480 and 482 either a "1" or a "0" bit is assembled with the preceding data bits, as appropriate. At step 484, the "dead period" timer (10 milliseconds) is reset and at step 470 program operation returns to the main loop.

Referring now to the DECODE subroutine of FIG. 13B, the first step 490 is to determine whether a complete word has been received. This determination is made upon occurrence of a "dead" period by checking the bit count and comparing that current count with the length of the authorization code. If a complete word has not been received, then the subroutine returns to the main loop. If a complete word has been received, then at step 492, the received word is compared against the stored authorization codes to determine if there is a match. If not, the program operation returns to the main loop. If the received word matches any of the programmed authorization codes, then if the matching code has been received twice consecutively (step 494), the decoder is activated at step 496. If the matching code has not been received twice consecutively, program operation returns to the main loop without activating the decoder. The requirement that the matching code be received twice consecutively is a further security feature, against the user of code scanners.

A "dead period" timer is employed as a "background" function, which on an interrupt basis monitors the receiver output to locate 10 millisecond time periods between received data. Such gaps indicate that a data word has been received. The dead period finder function is illustrated in FIG. 13C. The routine employs a 10 millisecond software timer, which is reset during the bit assembler operation (step 484, FIG. 13A). At step 501, this dead period timer is checked to determine if it has received the "0" timed-out state. If not, the operation returns to the particular function in the main loop at which the interrupt occurred. If the timer state has reached "0", then at step 502, the bit count is checked to see if the bit count is not equal to the maximum possible code bit length. If the count equals that maximum length, then the decoder is reset to the inactive state at step 506, and the operation returns to the main loop. If the bit count does not exceed this maximum length, then the error flag is checked at step 503, and if set, operation branches to step 506 to reset the

4,887,064

17

decoder. If the error flag is not set, then at step 504, the assembled word is stored (step 504) in a buffer memory comprising the controller 70, the completed word timer is reset at step 505, the decoder is reset to the inactive state (step 506), and operation returns to the main loop.

The ALARM mode function (function 406 in FIG. 11) is shown in FIGS. 14A-D. This function is to activate and deactivate the alarm condition events at the appropriate times. At step 507, the alarm flag is checked. If set the alarm timer state is checked (step 508A) to determine whether it has reached the "0" or timed-out state. If the timer state is "0," then the ALARM, TRIPPED and PANIC flags are cleared (step 508B), the controller outputs for the controlled alarm devices are turned off (step 508C), and operation returns to the main loop. If the alarm flag is not set (step 507), the TRIPPED and PANIC flags are checked at step 509. If neither flag is set, no alarm devices are to be activated, and therefore operation returns to the main loop. If either the TRIPPED or the PANIC flag is set, then at step 510, the ALARM flag is set. At step 511, the alarm timer is loaded with the programmed alarm duration, and then the alarm outputs are turned on (step 512), including such controlled devices as, for example, the siren, pulsed alarm, autodialer and vehicle interior light. Steps 513 and 514 indicate the SIREN and PULSED ALARM subroutines, the former illustrated in FIGS. 14C-D. Operation then returns to the main loop.

The first step of the SIREN subroutine (FIG. 14B) is to determine whether the siren counter is at the "0" state (step 515). If not, the counter is decremented (step 516) and its state is again checked. If the count is "0," at step 525, the timer variable TSIREN is set to 240 milliseconds, the siren output line is turned off (step 526). Operation then returns to the main loop. If at step 515, the counter is at "0," then the siren counter is reset (step 521), TSIREN is set to 2.5 seconds (step 522) and the siren is turned on (step 523) before operation returns to the main loop. At step 517, if the counter state is not zero, then through step 518, either the OFFSOUND or ONSOUND subroutines (FIG. 14C and 14D, respectively) will be accessed. At step 520, operation for the next bit in the personalized siren code is set up, and operation returns to the main loop.

The first step 530 of the OFFSOUND routine (FIG. 14C) is to turn off the siren. The bit status of the programmed siren code is checked, and if it represents a dash, the TSIREN time variable is set to 720 milliseconds (step 532). Otherwise TSIREN is set to 240 milliseconds for a "dot." Operation then returns to step 520 (FIG. 14A).

The first step 540 of the ONSOUND routine (FIG. 14D) is to turn on the siren. The current siren code bit is checked, and if it represents a "dash," TSIREN is set to 720 milliseconds. Otherwise TSIREN is set to 240 milliseconds. Operation then returns (step 543) to step 520.

The SIREN subroutine therefore results in generation of the programmed personalized siren code at the appropriate time.

The CONTROL module is described in further detail with respect to FIGS. 15A-15D. At step 550 (FIG. 15A) the decoder is tested to determine if it is in the active state (step 498 of FIG. 13B). If not in the active state, then there is no decoder activity for the CONTROL module to respond to, and the operation returns to the main loop. If the decoder is active, then if it was

18

just activated since the prior pass through the main loop, the panic timer is started (2.5 seconds) at step 552, and at step 553 the ARMED flag is checked to determine whether the system is armed. If armed, the DISARM subroutine (FIG. 15B) is entered. Otherwise the ignition switch is checked for its status and if turned on, the control function is ended and operation returns to the main loop. If the ignition switch is not turned on, then the ARM subroutine (FIG. 15C) is entered. Upon completion of either the DISARM or ARM subroutines, the control function is ended, and operation returns to the main loop. If, at step 551, the decoder was not just deactivated, then at step 557 the panic timer status is checked, and if "0" the PANIC flag is set at step 1558. Operation then returns to the main loop.

Upon entry of the DISARM subroutine (FIG. 15B), if the tandem security mode has been selected (step 557), then the INSTANT flag is cleared (step 558), the tandem timer is reset (step 559), and operation returns. If the tandem security mode has not been selected, then at step 560 the ARMED flag is cleared. At step 561, the trigger and sensor flags are checked to determine whether any tampering has occurred during the ARMED mode. If none of these flags are set, then at step 562 the audible chirp counter is set to 1, and at step 565 the appropriate chirp(s) is sounded. If tampering is indicated, then at step 563 the chirp counter is set to 3, and at step 564, the point of intrusion indicated by the particular active flag or flags is loaded into the LED register for display by the LED control function (step 420 of FIG. 11). Thus, the system will sound a first predetermined audible message (here, one chirp) if no tampering was detected, and a second predetermined audible message (here, three chirps) if tampering was indicated. Further, the point of intrusion will be indicated by the LED flash code generated during the LED CONTROL function.

After sounding the appropriate number of chirps by the SOUND CHIRPS subroutine (FIG. 15C), which indicate audibly that tampering has or has not been detected, then at step 566 the vehicle power door system is activated to unlock the vehicle doors, the dome light is turned on (step 567) and operation returns to the main loop. Thus, upon disarming the system the vehicle doors are automatically unlocked, and the vehicle dome light is activated for a predetermined time interval or until the ignition switch is activated.

The SOUND CHIRPS subroutine is shown in FIG. 15C. If the system is determined to be in the PROGRAM mode (step 568A), then one chirp is sounded (step 569A), the chirp counter is decremented (step 569B) and the operation returns if the chirp counter state is zero, or otherwise loops back to step 569A. If the system is not in the PROGRAM mode, and if the CHIRP ENABLE flag is not set (step 568B), operation returns. If the flag is set, then operation proceeds to step 569A.

Upon entry of the ARM subroutine (FIG. 15D), at step 570, the controller gets the trigger and sensor inputs, i.e., checks the various flags corresponding to these devices, and at step 571 determines whether the "HI/LO" feature has been disabled. If so, then operation branches to step 573. Otherwise, the door triggers are masked out at step 572. At step 556 the remaining trigger and sensor flags (after the masking operation) are checked to determine whether any are active. If not active, then at step 576, the chirp count is set to 2. Otherwise the active trigger(s) is disabled, to allow the

system to be armed without the disabled sensor or trigger. This disabling takes place by storing the disabled sensor or trigger device identification, and thereafter ignoring the state of these identified devices each time the sensor and trigger lines are interrogated by the controller 70. At step 575 the chirp count is set to 4 indicating that a defective device has been bypassed. At step 577 the ARMED and INSTANT flags are set and the ENTRY DELAY flag is cleared. At step 578 the appropriate number of chirps is sounded, and at step 579 the door lock output line is activated to automatically lock the vehicle doors. Thus, the system automatically activates the door power locking system when the system is armed. Operation then returns to the main loop.

The DISARMED module (step 416 of FIG. 11) is shown in more detail in FIGS. 16A-E. At step 581, the HOOD subroutine (FIG. 16B) is entered. At step 582, the ignition switch is checked. If it is activated, then at step 583, a test is performed to determine whether the ignition switch was activated since the last pass through the subroutine. If yes, then at step 585, the door lock system is activated to lock the doors. At step 583, the PROGRAM QUALIFY subroutine is entered which begins a 10 second timer after the ignition switch is turned on, during which interval the ENTER PROG module (step 426 of FIG. 11) can be entered by toggling the program "valet" switch 77. At step 587 the EXIT DELAY flag is cleared, ending the exit delay during which the user is provided the opportunity to exit the vehicle without activating the alarm. Operation then returns to the main loop. If the ignition switch was not on at step 582, then the valet flag is checked at step 588. The operation then proceeds to step 486 to clear the EXIT DELAY flag. Otherwise, the passive arming flag is checked at step 590 to see if this feature is disabled, and if so, operation proceeds to step 586. If passive arming is not disabled, then at step 592 the RECORD subroutine is entered.

The HOOD subroutine is shown in FIG. 16B. At step 600, the status of the "hood" program switch (one of switches 77) is interrogated to determine whether the hood switch was just activated since the last pass through the subroutine. If yes, then the status of the hood release controlled device 96 is checked to see whether it is active (step 601). If active, it is turned off (step 602); if not active, the hood release device is turned on (step 603). Operation then returns. If the hood switch was not just activated (step 600), operation returns via step 604 if the hood release device is not active. If the hood release is active (step 604), the hood sensor is checked (step 605), and if open, operation returns. If not open, the determination is made at step 606 if the hood was closed since the last pass through the subroutine. If it was, a 30-second timer is started, and operation returns. If not, then at step 607, the 30 second timer is checked to determine whether it has timed out. If so, the hood release device is turned off, locking the hood, and operation then returns to step 582.

The RECORD subroutine is shown in FIG. 16C. The purpose of this routine is to record in the trigger/sensor register comprising the controller 70 any active triggers or sensors. Thus, at step 610, the ignition switch is checked to determine whether it was turned off since the last pass through the subroutine. If not, then operation returns. If so, then the contents of the trigger/sensor register maintained by the controller are accessed (step 611), and the door triggers are masked out at step

612. Then any active sensor or triggers, excepting the masked door triggers, are recorded in the register (step 613). The doors are unlocked (step 614) and operation then returns to step 594.

At step 594 of FIG. 16A, the door triggers are checked to determine whether the doors have been opened and closed. If not, operation proceeds to the UPDATE routine (FIG. 16E). Otherwise operation proceeds to the PASSIVE routine (FIG. 16D). In the latter routine, the exit delay timer is checked at step 620 to determine whether the exit delay is over. If it is, then at step 621, any triggers or sensors recorded in the trigger/sensor register are disabled, and at step 622 the ARMED flag is set. A determination is made as to whether the door was opened during the disarmed mode. If so, operation returns. If not, the door lock device 94 is activated to lock the doors (step 624). If the exit delay is not over (step 620), then at step 625 the contents of the trigger/sensor register are fetched, and at step 626 the contents of the "record" register are masked from the trigger/sensor register contents. If the result is a blank register, then the routine returns. Otherwise, the exit delay timer is reset before returning.

The UPDATE subroutine is illustrated in FIG. 16E. The purpose of this subroutine is to clear any bit in the record register that is inactive as illustrated in steps 630 and 631 in FIG. 16E.

The ARMED function 414 (FIG. 11) is illustrated in FIGS. 17A-F. The first step 640 (FIG. 17A) of this function is to determine the status of the triggers and sensors. At step 642, any sensors or triggers previously identified as disabled are masked out. The next steps 643-46 are to execute the subroutines DOOR, ENTRY, SENSOR and OTHER TRIGS which are shown in FIGS. 17B-E, so as to determine which active trigger or sensor elements should result in activating the alarm controlled elements. At step 647, the TRIPPED flag is checked, and if set, the SHUT OFF subroutine (FIG. 17F) is executed. Otherwise, the trip counter is reset (step 649) to 10. The purpose of the trip counter is to prevent alarms from continuing after ten successive passes due to the same trigger or sensor being active. This prevents noise pollution and conserves the vehicle battery. Operation then returns to the main loop.

Referring now to FIG. 17B, the DOOR subroutine is depicted. The door triggers are checked at step 651, and if not active (i.e., the door are closed), then the DOOR OK flag is set (step 652) and operation proceeds to the ENTRY subroutine. If a door trigger is active, then if the "HI/LO" feature is not disabled, the DOOR OK flag is checked. If not set, operation proceeds to the ENTRY subroutine. If the "HI/LO" feature is disabled, or if the DOOR OK flag is set, then the INSTANT flag is checked (step 655), and if set, the door trigger active status is interpreted as an alarm condition, the TRIP flag is set (step 656A) and the intrusion point is recorded (step 656B) before proceeding to the ENTRY subroutine. If the INSTANT flag is not set, then at step 657A, the ENTRY DELAY flag is set, the dome light is turned on at step 657B, and the entry delay timer is started at step 657C.

The ENTRY subroutine is shown in FIG. 17C. The ENTRY DELAY flag is checked (step 658), and if not set, operation proceeds to the SENSOR subroutine. If the flag is set and if the entry delay timer state is "0," then the TRIPPED flag will be set. Operation otherwise proceeds to the SENSOR subroutine.

4,887,064

21

The first step 661 of the SENSOR subroutine (FIG. 17D) is to check the five-second timer initiated when the system was armed. If the timer has not timed out, the sensor lines or bits are masked out (step 662) and operation proceeds to the OTHER TRIGS subroutine (FIG. 17E). If the timer has reached zero, then the sensor lines are checked (step 663), and if none are active, operation proceeds to the OTHER TRIGS subroutine. If a sensor is active, the TRIPPED flag is set (step 664), and operation proceeds to the OTHER TRIGS subroutine.

In the OTHER TRIGS subroutine (FIG. 17D), the triggers other than the door triggers are checked. If none are active, operation proceeds to step 647 (FIG. 17A). If any other triggers are active, the TRIPPED flag is set at step 668, and operation proceeds to step 647.

The SHUTOFF subroutine (FIG. 17F) is entered if the TRIPPED flag has been set. Here, the trip counter is decremented (step 672) and if its state is not zero, the intrusion point is recorded (step 674), and operation returns to the main loop. If the trip counter has reached zero, it is reset (step 675), the intrusion point trigger or sensor is disabled, and operation returns to the main loop. Thus, once the trip counter reaches its zero state, an alarm will not be generated as a result of the active trigger or sensor device on the next pass through the main loop.

The LED CONTROL function (step 420 of FIG. 11) is shown in further detail in FIGS. 18A-C. At step 680 (FIG. 18A), the ARMED flag is checked to determine whether the system is in the armed mode. If not armed, the IDENTIFY subroutine is entered at step 681. Otherwise, the DIAGNOSE subroutine is entered at step 682 and thereafter operation returns to the main loop.

The IDENTIFY subroutine is shown in FIG. 18B. At step 686, the controller determines whether an intrusion was attempted while the system was armed. If not, then the green LED is flashed (step 689) and operation returns to the main loop. If an intrusion was attempted, then at step 687, the message counter is checked, and if zero, the INTRUSION flag is cleared (step 689), the green LED is flashed, and operation returns to the main loop. If the counter is not zero, then it is decremented (step 690). At step 691 the point of intrusion is established by reading the flags associated with the activated triggers and sensors stored in the register. The proper LED pulse count corresponding to the intrusion point is set (step 692), and at step 693, the appropriate LEDs are turned on. At step 694 the voice synthesizer is activated to announce audibly the intrusion point. It will be appreciated that the voice synthesizer is programmed to provide a plurality of messages, and that a particular message may be chosen and activated in correspondence to a particular control signal from the controller. Such a selection may be accomplished by a look-up table function, as where a particular intrusion point code selects the appropriate message. Voice synthesizers are known in the art having the capability of generating a selected one of a plurality of stored messages. Operation then returns to the main loop.

The DIAGNOSE subroutine is shown in FIG. 18C. At step 695, the controller determines whether there is a disabled trigger or sensor. If not, at step 696, a red LED is flashed, and operation then returns to the main loop. If a sensor or trigger is disabled, then the message counter is checked (step 697), and if "0," the LED is flashed, and operation returns. Otherwise, the counter is

22

decremented (step 698), the data defining the disabled trigger or sensor is obtained (step 699), the proper pulse counter corresponding to the particular disabled sensor or trigger is set (step 700), and visible and audible messages identifying the disabled element are generated at steps 701 and 702 by the LED and voice synthesizer.

The ENTER PROG function (step 426 of FIG. 11) is shown in further detail in FIGS. 19A-L. At step 705, the 5 second program qualify timer (started at step 586, FIG. 16A) is checked. If its state has reached "0," operation returns to the main loop. If the counter has not reached "0," then the program "valet" switch is checked, and if toggled within one second, the PROGRAM MODE (FIGS. 19B-L) is entered at step 707.

The PROGRAM MODE subroutine 426 is illustrated in further detail in FIGS. 19A-L. The overall module is illustrated in FIG. 19B-C. Upon entering the module, the system sounds a chirp to signal to the user that the program mode has been entered (step 710), and at step 711, a ten-second timer is reset. The program switch is interrogated at 712. The program switch is toggled by the user to select a particular programming option. By way of example, toggling the switch three times may result in selecting the siren duration programming option. Other means for making a programming option selection may be employed, such as using a key pad to enter a predetermined code. The ignition switch must be on in this embodiment to perform any programming, and, if the ignition switch is not on (step 713), operation return to the main loop. The selection timer is checked to determine whether it has timed out (step 714), and if so, operation returns to the main loop. If the timer is not zero, then a determination is made whether a programming selection has been made via the program switch. If not, then operation loops back to step 712, until the timer expires. Once a selection is made, then the remainder of the subroutine comprises executing the selected programmable option. Thus, steps 716-726 consist of determining whether particular programmable options were selected. The selected option is then programmed via the appropriate one of the programming subroutines set forth in 727 and 729-739.

The first programming option indicated in FIGS. 19A-B is the TRANSMITTER CODE option (step 729) which enables the system to program a new transmitter authorization code. This feature is described more fully in the co-pending application, Ser. No. 094,395, described above.

The SIREN DURATION programmable option (step 730) allows the user to program the length of each siren alarm interval, for any length from 1 to 255 seconds. At step 740 (FIG. 19D), the system sounds two chirps alerting the user that the programming option has been selected. A siren duration timer is set to one second (step 741), and at step 742, the operation loops with the timer running, until the program switch is no longer in the position. At that point, the new duration value, i.e., the timer state, is recorded. The EXIT flag is set at step 744, and operation returns.

The SIRENTONE programmable option (step 731) is illustrated in further detail in FIG. 19E-F. The purpose of this module is to enable the user to program the system with a personalized siren code so that in the event of an alarm, the user may determine from a distance whether the audible alarm is emanating from his vehicle, and not from another vehicle, as for example, in the case where the vehicle is parked in a crowded parking lot or structure. At step 750, the system sounds two

chirps. At step 751, the program "valet" switch is checked to determine whether it is in the "on" position. If so, then at step 752 the LONG PAUSE flag is set. Otherwise the operation branches to step 753, where the program switch is checked. If it is not on, then the operation loops back to step 751. If the program switch is on, then at step 753, the TONE subroutine is entered (FIG. 19E). At step 755, the exit flag is checked, and if not set, operation loops back to step 751. If the exit flag is set, then operation returns to step 728.

The TONE subroutine (FIG. 19E) commences with a check of the program switch to determine whether it was held for 2.5 seconds (step 760). If not, then at step 761 the DOT flag is set. Otherwise, the DASH flag is set at step 762. At step 763 the system sounds a chirp, and at step 714 the ignition switch is checked. If it is on, then the counter is decremented at step 765. At step 766 the counter state is checked for the zero state and if not zero, the operation returns to step 755. If the ignition switch was not on at step 753, then the exit flag is set at step 767, and operation returns to step 755. This allows the user to program a personalized siren code made up of "dots" and "dashes."

The next programmable option is the HI/LO option (step 732). This feature allows the system installer to connect the door trigger line to the vehicle interior courtesy light switch, instead of a specially installed door trigger. This option per se forms no part of the present invention.

The next programmable option (step 733) is the PROG CHIRP option, shown in FIG. 19G. This option allows the system user to selectively disable the audible chirps which are sounded when the system is armed or disarmed. At step 775, the system sounds an appropriate selection chirp code, uniquely signifying that this option has been selected. At step 776, the momentary program switch is interrogated, and if active, the CHIRP DISABLE flag is set (step 777). If the momentary program switch is not active, then at the toggle program switch is interrogated. If it is not active, operation loops back to step 776. If the toggle program switch is active, then the CHIRP DISABLE flag is cleared (step 779).

The next programmable option is the PROG ENTRY option (step 734). This option enables the system user to program the entry timer duration, i.e., the time duration between opening the vehicle door and the entry of an appropriate code to disable the alarm. A similar programmable option is the PROG EXIT option (step 735). This option enables the system user to program the duration of the exit delay, i.e., the time between actively initiating the arming of the system by closing the last vehicle door, and the actual arming of the system. This delay gives the user time to exit the vehicle and to close the vehicle doors without triggering the alarm. The PROG ENTRY and PROG EXIT features per se form no part of this invention.

The next programmable option is the DOOR PULSE option (step 736) shown in FIG. 19H. The purpose of this option is to enable the installer of the system to select the duration of the door lock and unlock controlled signals. In general, vehicle power door locking systems are actuated by either a one second or a three second pulse, depending on the vehicle manufacturer. In the past, alarm systems have required the use of an interface module to actuate the door locking system because of the two types of signals. With the invention, the system installer programs the system to provide the pulse width required for the particular vehicle. Thus, at

step 790, the door pulse width status is displayed, e.g., by activating a dedicated LED if the present status is to generate the long pulse, or not activating the status LED if the short pulse is selected. At step 791, the operation loops until new keys have been selected. If the new key is the key needed to exit this programmable option, then the door pulse width status is stored in the controller memory (step 795), and operation returns. If the new key selected is the door pulse key, then the pulse width status is toggled (step 794) and operation return to step 790. The result is that the controller 70 will activate the appropriate output control line for the "door lock" and "door unlock" functions when appropriate for the selected time duration, here either one or three seconds.

The next programmable option is the DOOR POLARITY option (step 737), shown in FIG. 19I. This allows the system to be programmably adapted to a door trigger device having either positive or negative polarity. Thus, with the driver's door opened, thereby activating the door trigger, the controller checks the door trigger line (step 800), and if low or "0," the positive POS DOOR flag is cleared (step 803); otherwise, the positive POS DOOR flag is set (step 802). This allows the installer to connect the door trigger to a predetermined terminal of the input buffer 80 without regard to the particular polarity of the trigger, thereby simplifying the installation.

The next programmable option is the PROG KBCODE option (step 738), shown in FIG. 19J. This option enables the system user to program a new user authorization code into the system via the key pad. For the sake of example, the user authorization code bit length is 5 bits. Then, at step 810, the code bit length counter is set to 5, and if a digit key on the keypad is pressed (step 811), this new code digit is stored in a temporary register (step 812). The counter is decremented at step 813, and if the resulting counter state is not "0" (step 814), and the exit key for exiting this option is not active (step 816), the operation loops back to step 811. If the counter has reached the "0" state, indicating that a complete code word has been entered (step 814), the new code is stored in memory (step 815) and operation returns (FIG. 19B).

The next programmable option is the TRIG BY-PASS option (step 739), shown in FIG. 19K. This option enables the system user to selectively bypass defective sensor or triggers, thereby allowing the system to be used even though one or more triggers or sensors may be defective. Thus, the sensors and triggers may be either selectively bypassed by the user, or automatically bypassed, as discussed above. At step 820 the key pad keys are interrogated. All disabled triggers and sensors are visually displayed, e.g., by utilizing the appropriate key pad LED. If the key for exiting this option is activated at step 822, operation returns. Otherwise, if there are no other active keys, operation loops back to step 820. If there are active keys, then at step 824, the enabled/disabled status of the trigger or sensor corresponding to the active key is obtained. If that trigger or sensor is disabled, its status is changed to the enabled state (step 827). If the particular trigger or sensor is not disabled, then its status will be changed to the disabled state (step 826).

The final programmable option for this embodiment is the TANDEM option (step 727), shown in FIG. 19L. This provides the user with the capability of selecting the level of security provided by the system, in that the

4,887,064

25

user selects the disarming functions required as either (1) entry of the authorization code via the transmitter, or (2) entry of the authorization code via the transmitter and subsequent manual entry of the authorization code via the keypad. Thus, access to the vehicle or secured area when the latter alternative is selected requires that the user have the transmitter and also know the key pad authorization code. Once the programmable option is selected, the present security status is displayed (step 830), i.e., whether or not the tandem disarming functions are selected. The display may be via a dedicated LED which is activated only if the "tandem" security mode has been selected. The operation then essentially "waits" until a new keypad key is selected. If the new key is that key for exiting the option, then the security status is stored and operation returns. If the new key is the key for changing the security status (step 833), then the security status is toggled (step 834), and operation returns to step 830.

The system sounds three chirps at step 728, indicate to the user that the PROGRAM MODE has been exited. Operation then returns to the main loop.

The BATTERY CHECK function module is shown in FIG. 20. This module prevents the system from draining the battery when an alarm condition is detected. Thus, at step 840, the error signal from the 5 volt power supply (node E, FIG. 6) is tested to determine whether it is active, signifying that the 5 volt supply is not available, and if so, the tripped flag is cleared and the operation returns to the main loop. Thus, no matter what the condition of the system, the low battery voltage results in clearing the alarm status.

The DOME LIGHT function module is shown in FIG. 21. The purpose of this module is to provide the capability of turning the vehicle courtesy light on and leaving it on for a predetermined period of time after the system has been disarmed. At step 845, the dome light output line of the controller is checked, and if not on, then at step 846 the controller determines whether the vehicle driver's door was just opened. If not, then operation returns to the main loop. If the door was just opened, then the dome timer is reset at step 847, and the dome light output is turned on by the controller at step 848. If at step 845, the dome output is on, then the ignition is checked at step 849, and if not on, then the dome timer is checked and if not zero, the operation returns to the main loop. Otherwise, the controller dome output is turned off (step 851).

The next function performed during the main loop (FIG. 11) is the ENGINE CONTROL function (step 434), shown more fully in FIG. 22. This function allows the vehicle engine to be disabled from unauthorized starting. At step 855 the ENGINE DISABLE flag is checked, and if not set, operation returns to the main loop. If the flag is set, then at step 856, the ignition switch is checked to determine whether the engine is running. If it is running, operation returns to the main loop. If the engine is not running, then at step 857, the ENGINE DISABLE controller output is turned on. This is coupled to the engine, e.g., to a bypass relay on the engine starter, to disable the engine starting function. Thus, this function is only activated if the vehicle ignition is turned off, preventing a possible hazard arising from inadvertent ignition bypass when the vehicle is in operation.

The KEYBOARD CODE function is shown in FIG. 23. If a keyboard or key pad key is not determined to be actuated (step 860), operation returns to the main loop.

26

If a key is activated, then the "good digit" time is checked (step 861). This timer requires that successive digits be entered within a predetermined time interval. If the timer is zero, the digit counter index is set to "1" (step 862). At step 863, the entered digit is compared with the Nth digit of the key pad authorization code. If the entered digit is not the same, the good digit timer is set to zero, and operation returns to the main loop. If the entered digit is the same as the Nth code digit, then at step 865, the counter is checked, and if not equal to the number of bits in the authorization code (here 5), the timer is reset (step 866), and the counter is incremented at step 867 before operation returns to the main loop. If, at step 865, the counter index equals the code length, then the ARMED flag is cleared (step 868) and the PROG QUALIFY timer is reset (step 869).

It is understood that the above-described embodiments are merely illustrative of the possible specific embodiments which may represent principles of the present invention. Other arrangements may readily be devised in accordance with these principles by those skilled in the art without departing from the scope of the invention.

What is claimed is:

1. A security system for monitoring and controlling access to a protected area and having self-diagnostic capability, comprising:

a plurality of sensor devices, each for sensing an intrusion event and providing a sensor activated signal when the event is detected;

means for communicating alert signals;

a controller for controlling the operation of said security system so that said system may be operated in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue an alert signal in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating alert signals, said controller comprising:

(i) means for monitoring the state of each of said sensor devices;

(ii) means responsive to a system arming signal when the system is in the disarmed mode for identifying any sensor device providing a sensor activated signal; and

(iii) means for bypassing each of said identified sensor devices and placing the system in the armed mode wherein the state of said bypassed sensor devices does not prevent the system from being armed and wherein said bypassed sensor devices will not cause activation of said communicating means during said armed mode.

2. The security system of claim 1 wherein said sensor device identifying means comprises means for providing a visual signal indicative of said identified sensor device providing a sensor activated signal.

3. The system of claim 1 wherein said bypassing means of said controller automatically bypasses predetermined ones of said identified sensor devices without system user intervention.

4. The security system of claim 1 wherein said sensor device identifying means comprises means for generating a voice synthesized audio signal indicative of said identified sensor device.

5. The security system of claim 1 further comprising user-operated means for communicating with said controller, said user-operated communicating means comprising means for selectively providing a bypass signal

27

4,887,064

to said controller indicating that selected ones of said identified sensor devices are to be bypassed.

6. The security system of claim 5 wherein said user-operated communicating means comprises a key pad accessible to a user for entering data to the system controller, and wherein said sensor device identifying means further comprises means for providing a visual identifying signal to a user indicative of the identified sensor providing a sensor device activated signal.

7. The security system of claim 1 wherein said controller further comprises means responsive to sensor activated signals and to user activation signals, said user activation signals for changing the system mode from the armed mode to the disarmed mode, for generating an indication signal that an unauthorized intrusion into said protected area has been attempted.

8. The security system of claim 7 wherein said indication signal comprises an audible signal, and said means for generating an indication signal further comprises means for providing a visual signal indicative of the particular intrusion point.

9. The security system of claim 7 wherein said indication signal comprises a visible indication signal identifying the particular intrusion point.

10. The security system of claim 1 wherein said means for generating alert signals comprises means for generating audible alert signals, and wherein said controller further comprises means for generating alert control signals which determine the duration of said audible alert signals during an alarm condition, and user programmed means activated during a system programming mode for receiving user-programmed duration signals which determine the duration of said audible alert signals during said alarm condition.

11. The security system of claim 10 further comprising a user-activated data input means for providing said duration signals to said controller during said programming mode.

12. The security system of claim 1 wherein said means for generating alert signals comprises means for generating audible alert sounds, and wherein said controller further comprises means for generating control signals for controlling said audible sound generating means to generate audible alert signals during an alarm signal cycle, and user programmable means activated during a system programming mode for receiving user-programmed code signals, said alert code signals capable of defining a distinctive user-personalized pattern of audible alert sounds corresponding to said code signals, and said controller is responsive to said code signals for generating user-personalized control signals in dependence on said user-programmed code signals, thereby causing said alert signal generating means to generate a user-personalized distinctive pattern of audible alert signals during said alarm cycle duration.

13. The security system of claim 12 wherein said user-personalized pattern of audible sounds takes the form of a distinctive pattern of audible "dots" and "dashes".

14. The security system of claim 12 wherein said means for generating audible alert signals comprises a siren device, and said audible sounds take the form of a user-personalized siren code made up of audible "dots" and "dashes".

15. The security system of claim 12 further comprising a user-activated data input means for providing said code signals to said controller during said programming mode.

28

16. The security system of claim 1 wherein at least one of said sensor devices is of the type wherein said sensor activated signal is either a first polarity output signal or a second polarity output signal, said sensor device providing an output signal of a particular one of said polarities as said sensor activated signal, and wherein said monitoring means of said controller is polarity programmable during a system programming mode to selectively recognize for said sensor device said particular polarity output signal as said sensor activated signal.

17. The security system of claim 16 further comprising means for putting said system in a system programming mode for sensor polarity programming, means for activating said sensor to simulate an intrusion event, and wherein said controller further comprises means for reading the state of said sensor device output signal during said programming mode and programming means responsive to said state of said sensor device output signal for recording and recognizing said output state as said sensor activated signal.

18. The system of claim 1 further comprising audio signal means for generating a first audio signal indicative of the armed mode when the system is toggled from the disarmed mode and a second audio signal indicative of the disarmed mode when the system is toggled from the armed to the disarmed mode, and further comprising user programmable means operable during a system programming mode for selectively disabling said audio signal means, whereby said system may be selectively programmed to toggle between said armed and disarmed modes without providing said audio signals.

19. The system of claim 1 wherein said protected area comprises the interior of a vehicle, and said vehicle further comprises a power door locking and unlocking system for locking the vehicle door or doors in response to a "door lock" signal and for unlocking the doors in response to a "door unlock" signal, and wherein said controller further comprises means for providing said "door lock" signals to said power locking and unlocking system in response to the toggling of the system from the disarmed mode to the armed mode, means for providing said "door unlock" signals in response to the toggling of the system from the armed mode to the disarmed mode, and programmable means for selecting the duration of said "door lock" and "door unlock" signals during a system programming mode to match the security system to the particular power door locking and unlocking system.

20. The security system of claim 19 further comprising installer-activated means for putting said system in a system programming mode for selection of said signal duration, and said means for providing said "door lock" signal comprises first means for generating said "door lock" signals having a first predetermined duration and second means for generating said "door lock" signals having a second predetermined duration, said means for providing said "door unlock" signals comprises first means for providing said "door unlock" signals having a first predetermined duration and second means for providing said "door unlock" signals having a second predetermined duration, and said programmable means comprises installer-activated switch for selecting at will either said first respective means or said second respective means.

21. The security system of claim 19 further comprising installer-activated switch for putting said system in a system programming mode for selection of said signal

duration, and said programmable means comprises installer-activated switch for selecting a first signal duration or a second signal duration.

22. The security system of claim 21 wherein said first signal duration is about one second, and said second signal duration is about three seconds.

23. A vehicle security system for generating a user-personalized audible alert signal in the event an intrusion event is detected, comprising:

at least one sensor device for sensing an intrusion event and providing a sensor activated signal when the event is detected;

means for communicating audible alert signals for an alarm cycle duration in response to alert control signals;

a controller for controlling the operation of said security system so that said system may be operated in an armed mode wherein said controller monitors said at least one sensor device and causes said communicating means to issue an alert signal in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating alert signals, said controller comprising:

(i) user programmable means activated during a system programming mode for receiving and storing user-programmable alert code signals, said alert code signals capable of defining a distinctive user-personalized pattern of audible alert signals corresponding to said alert code signals; and

(ii) means responsive to said sensor activated signals for generating said alert control signals in dependence on said user-programmed alert code signals, thereby causing said alert communicating device to generate a distinctive pattern of user-personalized audible alert signals during said alarm cycle duration.

24. The security system of claim 23 wherein said user-personalized pattern of audible alert signals take the form of distinctive patterns of audible "dots" and "dashes."

25. The security system of claim 23 wherein said controller activates said alert communicating signals for a particular alarm period in response to a sensor activated signal, and said controller further comprises user programmed means activated during a system programming mode for receiving user-programmed siren duration signals for defining the duration of said alarm period.

26. The vehicle security system of claim 23 wherein said means for communicating audible alert signals comprises a siren device, and said audible sounds take the form of user-personalized audible siren code comprising audible "dots" and "dashes."

27. The vehicle security system of claim 23 further comprising a user-activated data input means for providing said alert code signals to said controller during said programming mode.

28. A security system for monitoring and controlling access to a vehicle, comprising:

at least one sensor device for sensing an intrusion event and providing a sensor activated signal when the event is detected;

means for communicating alert signals;

a power source for supplying voltage at a predetermined level to said security system;

means for monitoring the voltage level of said power source and generating a voltage error signal when

said predetermined voltage level is not available to said system;

a user-activated switch device for providing a switch signal when activated;

a controller for controlling the operation of said security system so that said system may be operated in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue an alert signal in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating alert signals, said controller further comprising means responsive to receipt and termination of said error signal and to said switch signal for causing an alert signal to be communicated after receipt and termination of said error signal if said switch signal is not present upon termination of said error signal.

29. The vehicle security system of claim 28 wherein said vehicle comprises an ignition switch having at least "on" and "off" positions, and wherein said user-activated switch device comprises said ignition switch, whereby disconnection of said power supply from the system will result in communication of an alert signal upon reconnection of said power supply at said predetermined voltage level unless said ignition switch is in the "on" position.

30. A vehicle security system for monitoring and controlling access to a vehicle, comprising:

at least one sensor device for sensing an intrusion event and providing a sensor activated signal when the event is detected, said sensor device being of the type wherein said sensor activated signal is either a first polarity output signal or a second polarity output signal, said sensor device providing an output signal of a particular one of said polarities as said sensor activated signal;

means for communicating alert signals;

a controller for controlling the operation of said security system so that said system may be operated in an armed mode wherein said controller monitors said sensor device and causes said communicating means to issue an alert signal in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating alert signals, said controller comprising:

(i) means for monitoring the state of each of said sensor devices; and

(ii) means for polarity programming said monitoring means during a system programming mode to selectively recognize for said sensor device said particular polarity output signal as said sensor activated signal.

31. The vehicle security system of claim 30 wherein said sensor device is a door trigger for providing binary-valued output signals indicating the open/closed status of one or more vehicle doors, said sensor activated signal indicating the open status of said door.

32. The vehicle security system of claim 30 further comprising means for putting said system in a system programming mode for programming the polarity of said sensor device, means for activating said sensor to generate said sensor activated signal during said programming mode, and wherein said controller further comprises means for reading the state of said sensor device output signal during said programming mode and programming means responsive to said state of said sensor device output signal for recording and recognizing

ing said output signal state as said sensor activated signal.

33. A security system for monitoring and controlling access to a protected area and having self-diagnostic capability, comprising:

- a plurality of sensor devices, each for sensing an intrusion event and providing a sensor activated signal when the event is detected;
- means for communicating alert signals;
- a controller for controlling the operation of said security system so that said system may be operated in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue an alert signal in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating alert signals, said controller comprising:
 - (i) means for monitoring the state of each of said sensor devices;
 - (ii) means responsive to a system arming signal when the system is in the disarmed mode for identifying any sensor providing a sensor activated signal;
 - (iii) means for bypassing each of said identified sensor devices and placing the system in the armed mode wherein the state of said bypassed sensor devices does not prevent the system from being armed and wherein said bypassed sensor devices will not cause activation of said communicating means during said armed mode; and
 - (iv) means responsive to sensor activated signals and to user activation signals for generating an indication signal that an unauthorized intrusion into said protected area has been attempted, said indication signal comprising an audio signal indicative of the particular intrusion point.

34. The security system of claim 33 wherein said means for generating an indication signal comprises a voice synthesizer for generating an audible voice message indicative of the particular intrusion point.

35. A security system for monitoring and controlling access to a protected area and having self-diagnostic capability, comprising:

- a plurality of sensor devices, each for sensing an intrusion event and providing a sensor activated signal when the event is detected;
- means for communicating alert signals;
- a controller for controlling the operation of said security system so that said system may be operated in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue an alert signal in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating alert signals, said controller comprising:
 - (i) means for monitoring the state of each of said sensor devices;
 - (ii) means responsive to a system arming signal when the system is in the disarmed mode for identifying any sensor providing a sensor activated signal; and
 - (iii) means for bypassing each of said identified sensor devices and placing the system in the armed mode wherein the state of said bypassed sensor devices does not prevent the system from being armed and wherein said bypassed sensor devices will not cause activation of said communicating means during said armed mode;

a portable transmitter device for transmitting information encoded RF signals;

a receiver device mounted in said protected area for receiving and decoding said information-encoded RF signals and providing decoded signals indicative of said encoded information;

first user-activated means located within said protected area for manually entering a predetermined user authorization code into the system; and
second user-activated means for selecting a first disarming mode or a second disarming mode during a system programming mode; and

wherein said controller further comprises:

- (i) a first disarming means responsive to said decoded signals for toggling the system mode from the armed mode to the disarmed mode;
- (ii) a second disarming means responsive to said decoded signals and said user authorization code for toggling the system mode from its present armed mode or disarmed mode to the other mode in dependence upon receipt of said decoded signals and subsequent receipt of said user authorization code within a predetermined time interval; and
- (iii) means for selecting either said first or second disarming means in dependence on said selected disarming mode such that said first disarming means is activated while said first disarming mode is selected and said second disarming means is activated while said second disarming mode is selected.

36. A vehicle security system, comprising:

a plurality of sensor devices, each for sensing an intrusion event involving the vehicle and providing a sensor activated signal when the event is detected;

means for communicating alert signals;

power supply means for supplying electrical power to said system;

means for detecting the disabling of power to said system;

a user-activated switch device for providing a switch signal to said controller;

a controller for controlling the operation of said security system so that said system may be operated in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue an alert signal in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating alert signals, said controller comprising:

- (i) means for monitoring the state of each of said sensor devices;
- (ii) means responsive to a system arming signal when the system is in the disarmed mode for identifying sensor devices providing a sensor activated signal;
- (iii) means for bypassing identified sensor devices and placing the system in the armed mode wherein the state of said bypassed sensor devices does not prevent the system from being armed and wherein said bypassed sensor devices will not cause activation of said communicating means during said armed mode; and
- (iv) means responsive to said detecting means and to said switch signal for causing said alert signal to be communicated when power is restored to said system after said disabling of power unless said switch signal is present upon restoration of

33

power to said system, whereby disabling of power to said system will result in communication of an alert signal upon restoration of power unless said switch device is activated to provide said switch signal to said controller, and no alert signal will be generated upon restoration of power if said switch device is activated.

37. A vehicle security system, comprising:

a plurality of sensor devices, each for sensing an intrusion event involving the vehicle and providing a sensor activated signal when the event is detected; means for communicating alert signals;

a controller for controlling the operation of said security system so that said system may be operated in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue an alert signal in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating alert signals, said controller comprising:

(i) means for monitoring the state of each of said sensor devices;

(ii) means responsive to a system arming signal when the system is in the disarmed mode for identifying sensor devices providing a sensor activated signal, said means comprising a light source and means for activating said light source to provide a light flash code indicative of said identified sensor providing said sensor activated signal; and

(iii) means for bypassing identified sensor devices and placing the system in the armed mode wherein the state of said bypassed sensor devices does not prevent the system from being armed and wherein said bypassed sensor devices will not cause activation of said communicating means during said armed mode.

38. A security system for monitoring and controlling access to a protected area and having self-diagnostic capability, comprising:

a plurality of sensor devices, each for sensing an intrusion event and providing a sensor activated signal when the event is detected; means for communicating alert signals;

power supply means for supplying power to said system;

means for detecting the disabling of said power to said system and generating an error signal when said power disabling is detected;

a user-activated switch device for providing a switch signal to said controller;

a controller for controlling the operation of said security system so that said system may be operated in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue an alert signal in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating alert signals, said controller comprising:

(i) means for monitoring the state of each of said sensor devices;

(ii) means responsive to a system arming signal when the system is in the disarmed mode for identifying any sensor device providing a sensor activated signal;

(iii) means for bypassing each of said identified sensor devices and placing the system in the armed mode wherein the state of said bypassed

4,887,064

34

sensor devices does not prevent the system from being armed and wherein said bypassed sensor devices will not cause activation of said communicating means during said armed mode; and

(iv) means responsive to said error signal and to said switch signal for causing said alert signal to be communicated when power is restored to said system after said disabling of power unless said switch signal is present upon restoration of power to said system, whereby disabling of power to said system will result in communication of an alert signal upon restoration of power unless said switch device is activated to provide said switch signal to said controller.

39. The security system of claim 38 wherein said protected area comprises a vehicle having an engine and an ignition switch having at least "on" and "off" positions, and wherein said user-activated switch device comprises said ignition switch, whereby disconnection of said power supply from the system will result in communication of an alert signal upon reconnection of said power supply at said predetermined voltage level unless said ignition switch is in the "on" position.

40. A multi-function vehicle security system, comprising:

at least one sensor device for sensing an intrusion event and providing a sensor activated signal when an event is detected;

means for communicating alert signals;

a portable transmitter device for transmitting information-encoded RF signals;

a receiver device mounted in said vehicle for receiving and decoding said information-encoded RF signals and providing decoded signals indicative of said encoded information;

user-activated means mounted within said vehicle for manually entering a predetermined user authorization code into the system;

user-actuated means for selecting a first disarming mode or a second disarming mode during a system programming mode;

a controller for controlling the operation of said security system so that said system may be operated in an armed mode wherein said controller monitors said at least one sensor device and causes said communicating means to issue an alert signal in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating alert signals, said controller comprising:

(i) a first disarming means responsive to said decoded signals for toggling the system mode from the armed mode to the disarmed mode;

(ii) a second disarming means responsive to said decoded signals and said user authorization code for toggling the system mode from its present armed or disarmed mode to the other mode in dependence upon receipt of said decoded signals and subsequent receipt of said user authorization code within a predetermined time interval; and

(iii) means for selecting either said first or second disarming means in dependence on said selected disarming mode such that said first disarming means is activated while said first disarming mode is selected and said second disarming means is activated while said second disarming mode is selected.

41. The vehicle security system of claim 40 wherein said user-activated means mounted within said vehicle

4,887,064

35

comprises a keypad having a plurality of switch keys mounted thereon.

42. The vehicle security system of claim 40 wherein said user-activated means for selecting a first disarming mode or a second disarming mode during a system programming mode comprises a user-activated data input means for providing electrical data signals to said controller indicating entry of a programming mode in order to select either said first or said second disarming mode, and said means for selecting said either first or second disarming means is responsive to said electrical data signals to perform said selection during said programming mode.

43. A security system for monitoring and controlling access to a protected area and having self-diagnostic capability, comprising:

a plurality of sensor devices, each for sensing an intrusion event and providing a sensor activated signal when the event is detected;

means for communicating alert signals;

a controller for controlling the operation of said security system so that said system may be operated in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue an alert signal in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating alert signals, said controller comprising:

(i) means for monitoring the state of each of said sensor devices;

(ii) means responsive to a system arming signal when the system is in the disarmed mode for identifying any sensor device providing a sensor activated signal, said sensor identifying means comprising means for providing a visual signal indicative of said identified sensor device providing a sensor activated signal, comprising a light source and means for activating the light source to provide a light flash code indicative of said identified sensor device; and

(iii) means for bypassing each of said identified sensor devices and placing the system in the armed mode wherein the state of said bypassed sensor devices does not prevent the system from being armed and wherein said bypassed sensor devices will not cause activation of said communicating means during said armed mode.

44. A vehicle security system for monitoring and controlling access to a vehicle, comprising:

at least one sensor device for sensing an intrusion event and providing a sensor activated signal when the event is detected;

means for communicating alert signals;

a power door locking and unlocking system for locking the vehicle door or doors in response to a "door lock" signal and for unlocking the doors in response to a "door unlock" signal;

a controller for controlling the operation of said security system so that said system may be operated in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue an alert signal in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating alert signals, said controller comprising:

(i) means for providing said "door lock" signals to said power locking and unlocking system in response to the arming of the system;

36

(ii) means for providing said "door unlock" signals in response to the disarming of the system;

(iii) programmable means for selecting the duration of said "door lock" and "door unlock" signals during a system programming mode to match the security system to the particular power door locking and unlocking system of the vehicle.

45. The vehicle security system of claim 44 further comprising installer-activated means for putting said system in a system programming mode for selection of said signal duration, and said programmable means comprises installer-activated means for selecting a first signal duration or a second signal duration.

46. The vehicle security of claim 45 wherein said first signal duration is about one second, and said second signal duration is about three seconds.

47. The vehicle security system of claim 44 further comprising:

a portable transmitter device for transmitting information coded RF signals;

a receiver device mounted in said vehicle for receiving and decoding said information-encoded RF signals and providing decoded signals indicative of said encoded information; and

(i) arming means responsive to said decoded signals when the system is in the disarmed mode for placing the system in the armed mode; and

(ii) disarming means responsive to said decoded signals when the system is in the armed mode for placing the system in the armed mode.

48. A vehicle security system, comprising:

at least one sensor device for sensing an intrusion event and providing a sensor activated signal when the event is detected;

means for communicating alert signals in response to alert control signals;

a controller for controlling the operation of said security system so that said system may be operated in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue an alert signal of a predetermined duration in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating alert signals, said controller comprising:

means for generating alert control signals indicative of said predetermined duration during an alarm condition, and user programmed means activated during a system programming mode for receiving user-programmed alert duration signals for defining said alert control signals to determine said duration of said alert signals during said alarm condition.

49. A security system for monitoring and controlling access to a vehicle, comprising:

at least one sensor device for sensing an intrusion event and providing a sensor activated signal when the event is detected;

means for communicating alert signals;

a power source for supplying voltage at a predetermined level to said security system;

means for providing a reset signal upon application of power to said system;

a user-activated switch device for providing a switch signal when activated;

a controller for controlling the operation of said security system so that said system may be operated in an armed mode wherein said controller monitors

said at least one sensor devices and causes said communicating means to issue an alert signal in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating alert signals, said controller further comprising means responsive to receipt of said reset signal and to said switch signal for causing an alert signal to be communicated after receipt of said reset signal if said switch signal is not present upon receipt of said reset signal.

50. The vehicle security system of claim 49 wherein said vehicle includes an ignition switch, and said switch device comprises said vehicle ignition switch, whereby an alert signal will be communicated upon receipt of a reset signal unless an ignition switch signal is present.

51. A vehicle security system, comprising:

a plurality of sensor devices, each for sensing an intrusion event involving the vehicle and providing a sensor activated signal when the event is detected; means for communicating alert signals;

a controller for controlling the operation of said security system so that said system may be operated in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue an alert signal in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating alert signals, said controller comprising:

(i) means for monitoring the state of each of said sensor devices;

(ii) means responsive to a system arming signal when the system is in the disarmed mode for identifying sensor devices providing a sensor activated signal; and

(iii) means for bypassing identified sensor devices and placing the system in the armed mode wherein the state of said bypassed sensor devices does not prevent the system from being armed and wherein said bypassed sensor devices will not cause activation of said communicating means during said armed mode.

52. The security system of claim 51 wherein said sensor device identifying means further comprises means for providing a visual signal indicative of said identified sensor device providing a sensor activated signal.

53. The system of claim 51 wherein said bypassing means of said controller automatically bypasses each of said identified sensor devices without system user intervention.

54. The security system of claim 51 wherein said sensor device identifying means comprises means for generating a voice synthesized audio signal indicative of said identified sensor device.

55. The security system of claim 51 further comprising user-operated means for communicating with said controller, said user-operated communicating means comprising means for selectively providing a bypass signal to said controller indicating that selected ones of said identified sensor devices are to be bypassed.

56. The security system of claim 55 wherein said user-operated communicating means comprises a key pad accessible to a user for entering data to the system controller, and wherein said sensor device identifying means further comprises means for providing a visual identifying signal to a user indicative of the identified sensor device providing a sensor activated signal.

57. The security system of claim 51 wherein said controller further comprises means responsive to sensor activated signals and to a system disarming signal changing the system mode from the armed mode to the disarmed mode, said means for generating an indication signal that an unauthorized intrusion into said protected area has been attempted.

58. The security system of claim 57 wherein said indication signal comprises an audible signal.

59. The security system of claim 57 wherein said means for generating an indication signal further comprises means for generating a visible indication signal identifying the particular intrusion point.

60. The security system of claim 57 wherein said means for generating an indication signal comprises a voice synthesizer for generating an audible voice message.

61. The security system of claim 51 wherein said means for generating alert signals comprises means for generating audible alert sounds, and wherein said controller further comprises means for generating control signals for controlling said audible sound generating means to generate audible alert sounds during an alarm signal cycle, and user programmable means activated during a system programming mode for receiving user-programmed code signals, said alert code signals capable of defining a distinctive user-personalized pattern of audible alert sounds corresponding to said code signals, and said controller is responsive to said code signals for generating user-personalized control signals in dependence on said user-programmed code signals, thereby causing said alert signal generating means to generate a distinctive pattern of user-personalized audible alert signals during said alarm cycle duration.

62. The security system of claim 61 wherein said user-personalized pattern of audible sounds take the form of distinctive pattern of audible "dots" and "dashes."

63. The security system of claim 51 wherein said means for generating alert signals comprises means for generating audible alert signals, and wherein said controller further comprises means for generating alert control signals which determine the duration of said audible alert signals during an alarm condition, and user programmed means activated during a system programming mode for receiving user-programmed duration signals which determine the duration of said audible alert signals during said alarm condition.

64. The system of claim 51 further comprising audio signal means for generating a first audio signal indicative of the armed mode when the system is toggled from the disarmed mode and a second audio signal indicative of the disarmed mode when the system is toggled from the armed to the disarmed mode, and further comprising user programmable means operable during a system programming mode for selectively disabling said audio signal means, whereby said system may be selectively programmed to toggle between said armed and disarmed modes without providing said audio signals.

65. The security system of claim 51 wherein at least one of said sensor devices comprises means for providing an output signal state having respective high and low voltage states, and wherein a particular one of said output signal states represents said sensor activated signal for said sensor device, said system further comprising means for causing said sensor device to generate said sensor activated signal during a system programming mode, and wherein said monitoring means of said

4,887,064

39

controller is programmable during said system mode to recognize said particular output signal state as said sensor activated signal.

66. The security system of claim 63 wherein said vehicle includes one or more vehicle doors, and said at least one of said sensor devices comprises a door trigger for indicating the open/closed status of at least one vehicle door.

67. The system of claim 51 wherein said vehicle further comprises a power door locking and unlocking system for locking the vehicle door or doors in response to a "door lock" signal and for unlocking the doors in response to a "door unlock" signal, and wherein said

40

controller further comprises means for providing said "door lock" signals to said power locking and unlocking system in response to the toggling of the system from the disarmed mode to the armed mode, means for providing said "door unlock" signals in response to the toggling of the system from the armed mode to the disarmed mode, and programmable means for selecting the duration of said "door lock" and "door unlock" signals during a system programming mode to match the security system to the particular power door locking and unlocking system.

* * * * *

15

20

25

30

35

40

45

50

55

60

65



US005157375A

United States Patent [19]
Drori

[11] **Patent Number:** 5,157,375
 [45] **Date of Patent:** Oct. 20, 1992

[54] **ELECTRONIC VEHICLE SECURITY SYSTEM**

- [75] Inventor: Ze'ev Drori, Los Angeles, Calif.
- [73] Assignee: Clifford Electronics, Inc., Chatsworth, Calif.
- [21] Appl. No.: 637,378
- [22] Filed: Jan. 4, 1991

Related U.S. Application Data

- [60] Division of Ser. No. 277,959, Nov. 30, 1988, which is a continuation-in-part of Ser. No. 231,159, Aug. 11, 1988, Pat. No. 4,922,224, which is a continuation-in-part of Ser. No. 138,828, Dec. 28, 1987, Pat. No. 4,887,064.
- [51] Int. Cl.⁵ B60R 25/00
- [52] U.S. Cl. 340/429; 340/426; 341/176
- [58] Field of Search 340/426, 430, 429, 527, 340/528, 539, 825.31, 825.69; 341/176; 307/10.2

[56] **References Cited**

U.S. PATENT DOCUMENTS

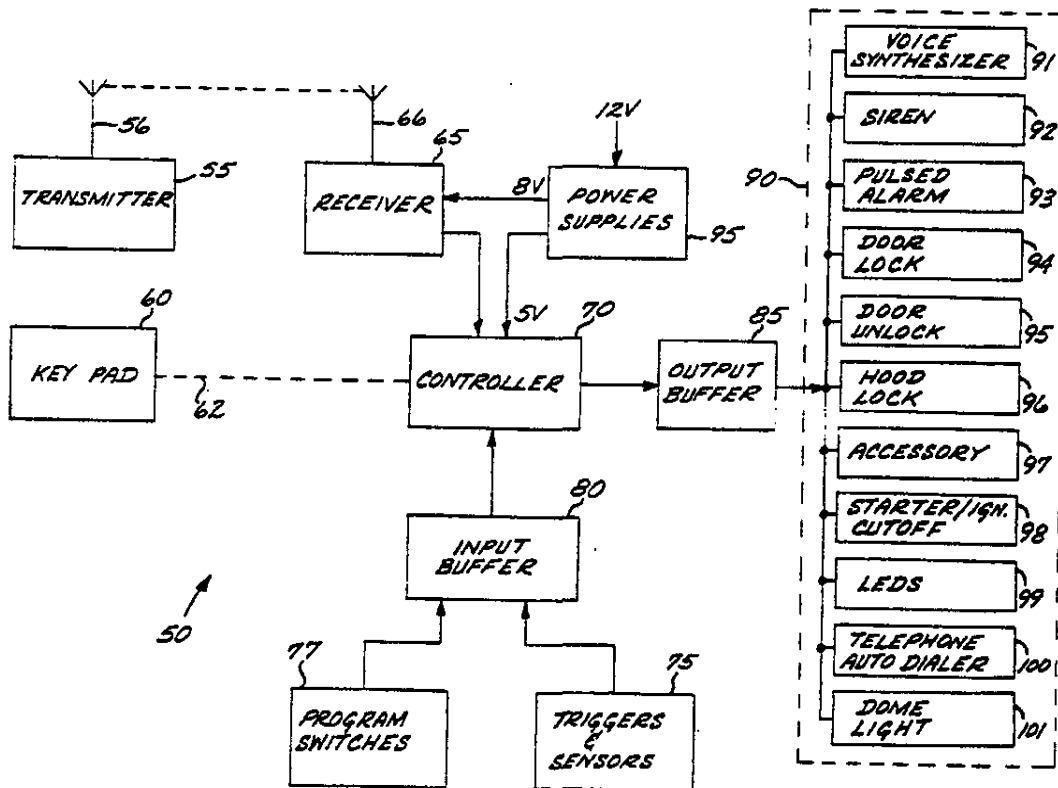
- 4,754,255 6/1988 Sanders et al. 340/426 X
- 4,794,368 12/1988 Grossheim et al. 340/527 X
- 4,897,630 1/1990 Nykerk 340/426
- 4,922,224 5/1990 Drori et al. 340/428

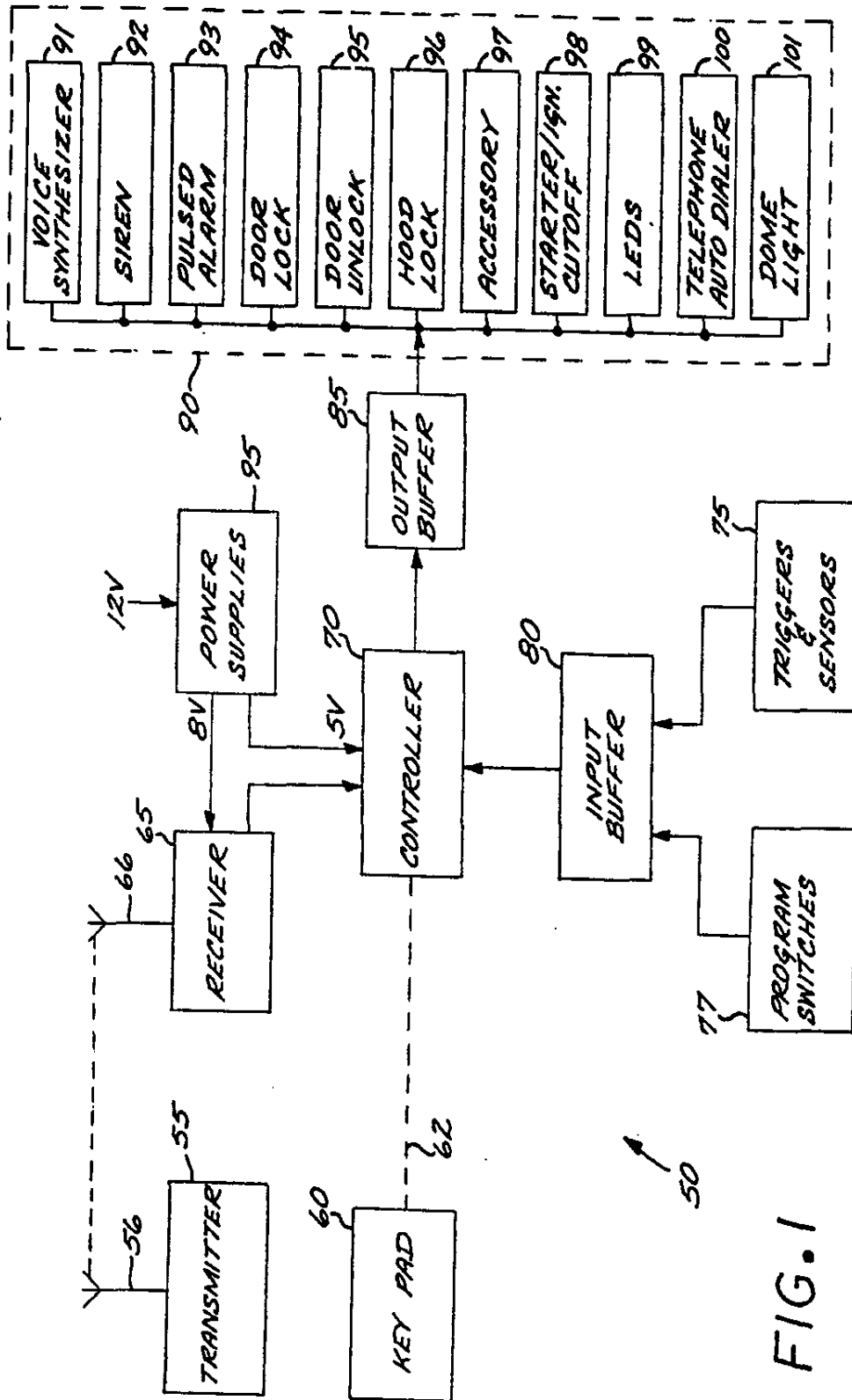
Primary Examiner—Jin F. Ng
 Assistant Examiner—Brian R. Tumm
 Attorney, Agent, or Firm—Roberts and Quiogue

[57] **ABSTRACT**

A multi-featured electronic vehicle security system is disclosed. The system is controlled by an electronic controller such a microcomputer. To reduce noise pollution due to false alarms caused by repetitive tripping of the system sensor devices, the system will not respond to more than a defined number of successive trippings of the same sensor device to initiate an alarm condition. The system includes a user-enabled feature wherein a first alarm signal generator is activated by a sensor tripping, and a second, distinct alarm signal generator is activated when a trigger device has been tripped. When the system is passively armed, active sensors and triggers are automatically diagnosed and bypassed, permitting the system to be passively armed even if one or more trigger or sensor is active. The system can be programmed so that if the system is disarmed by a remote control and the doors are automatically unlocked, the system will automatically rearm and relock the doors if a door is not opened within a predetermined time interval after disarming with the remote control.

15 Claims, 49 Drawing Sheets





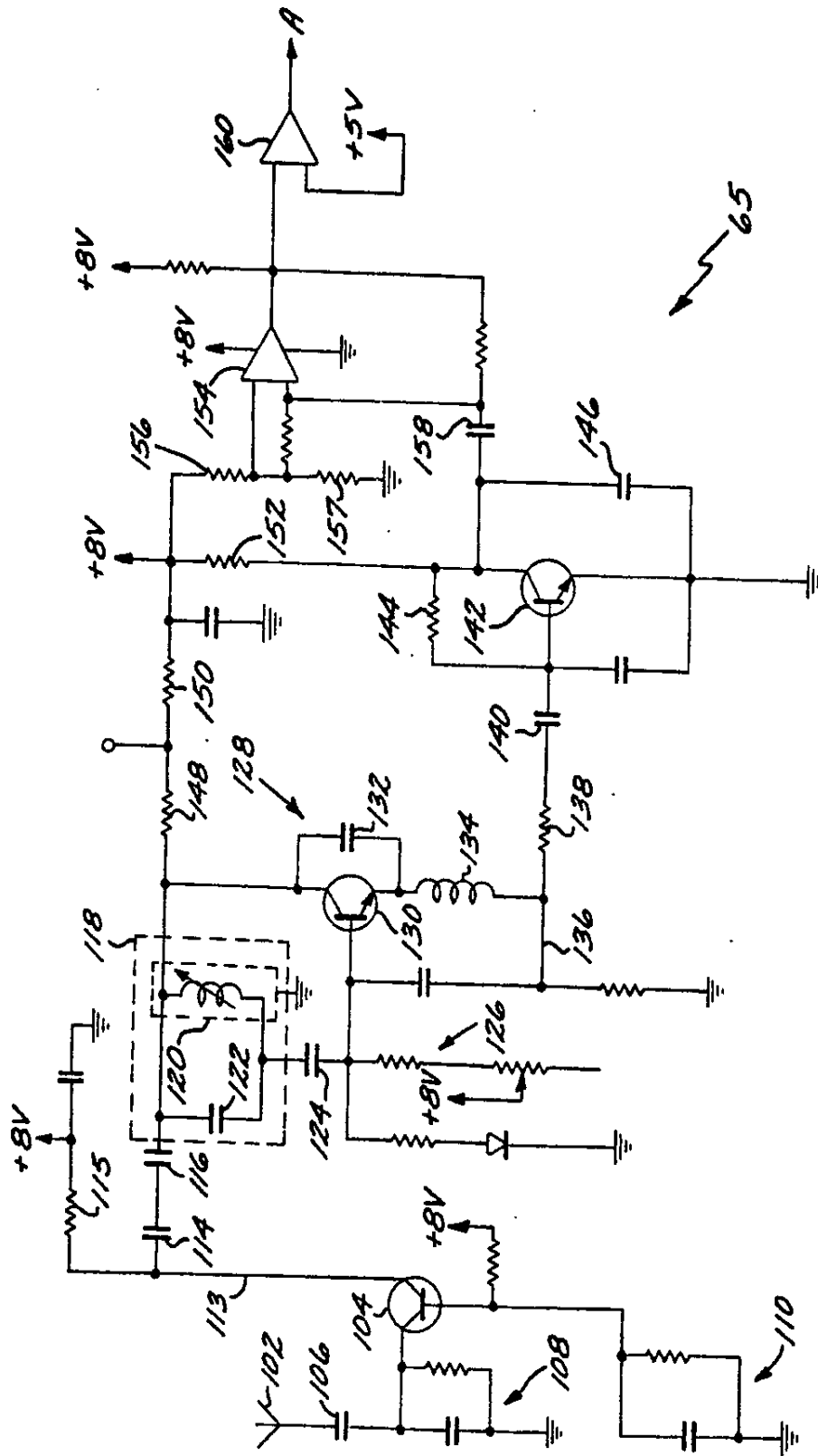


FIG. 2

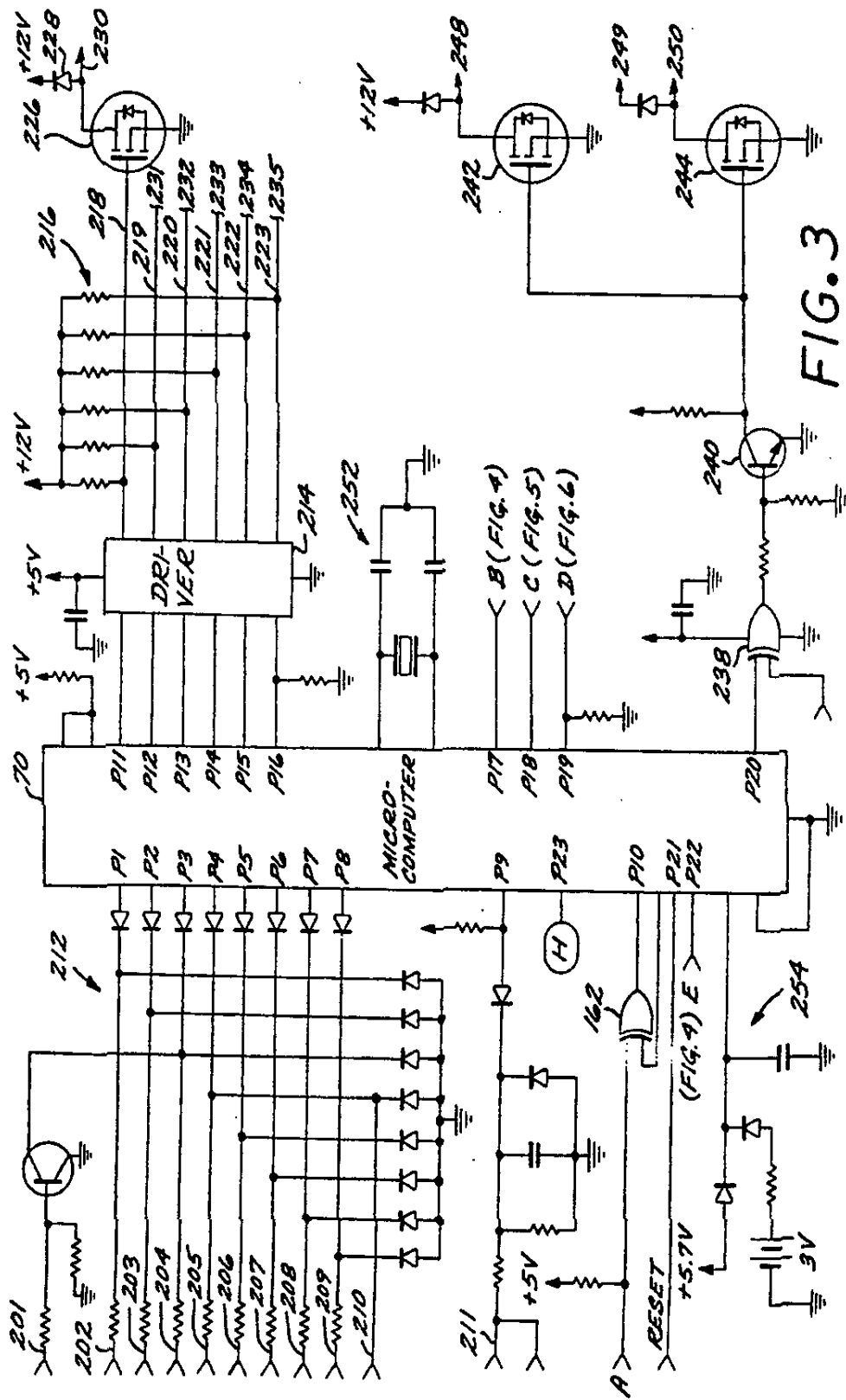


FIG. 3

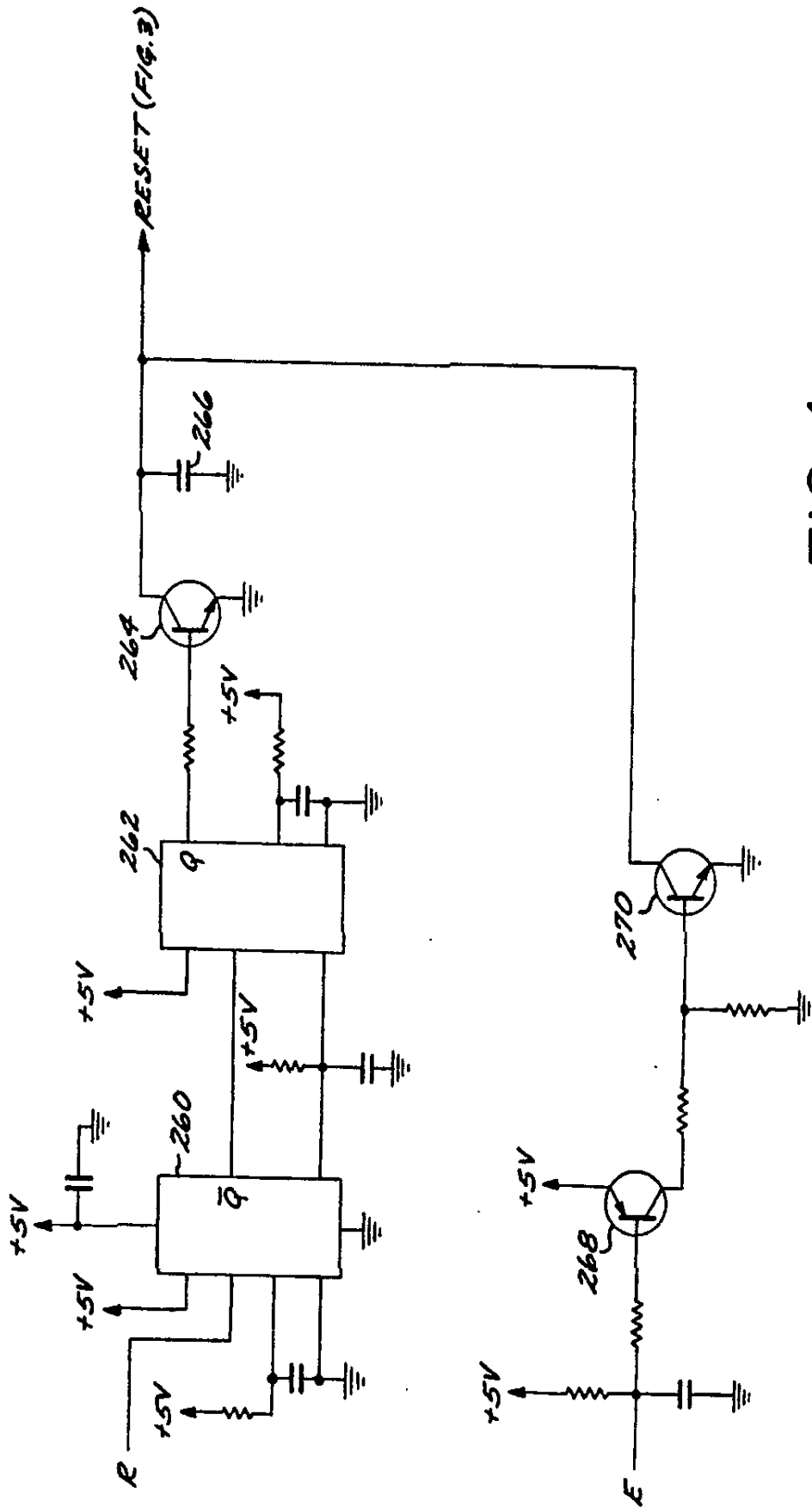


FIG. 4

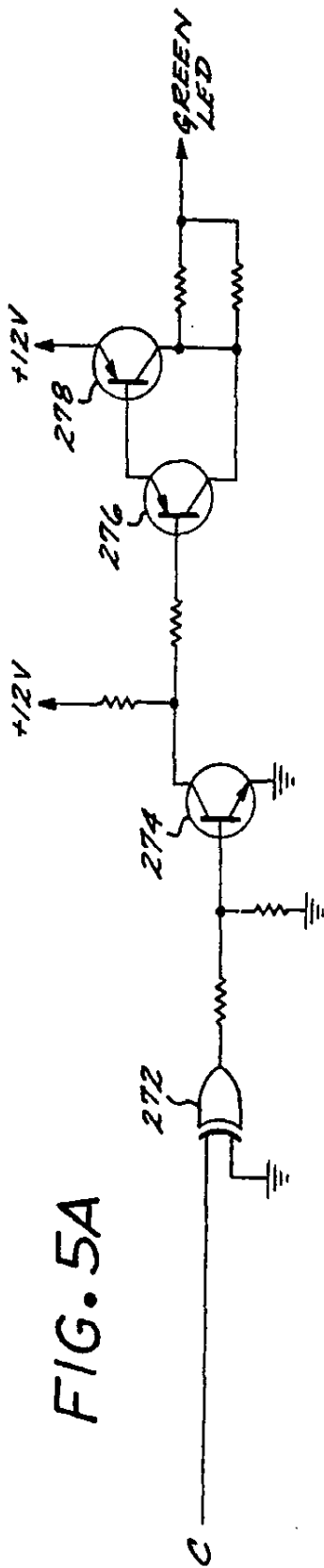


FIG. 5A

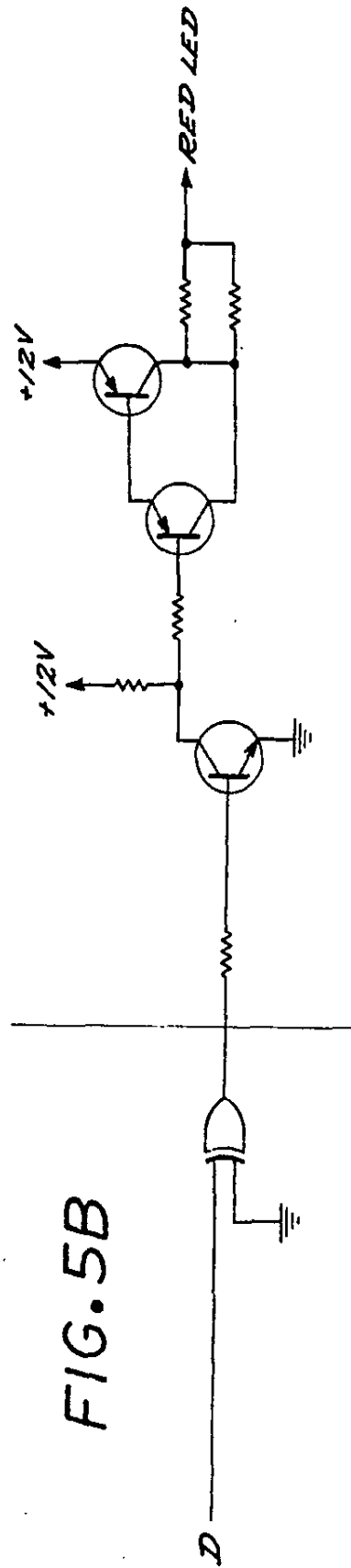


FIG. 5B

FIG. 6

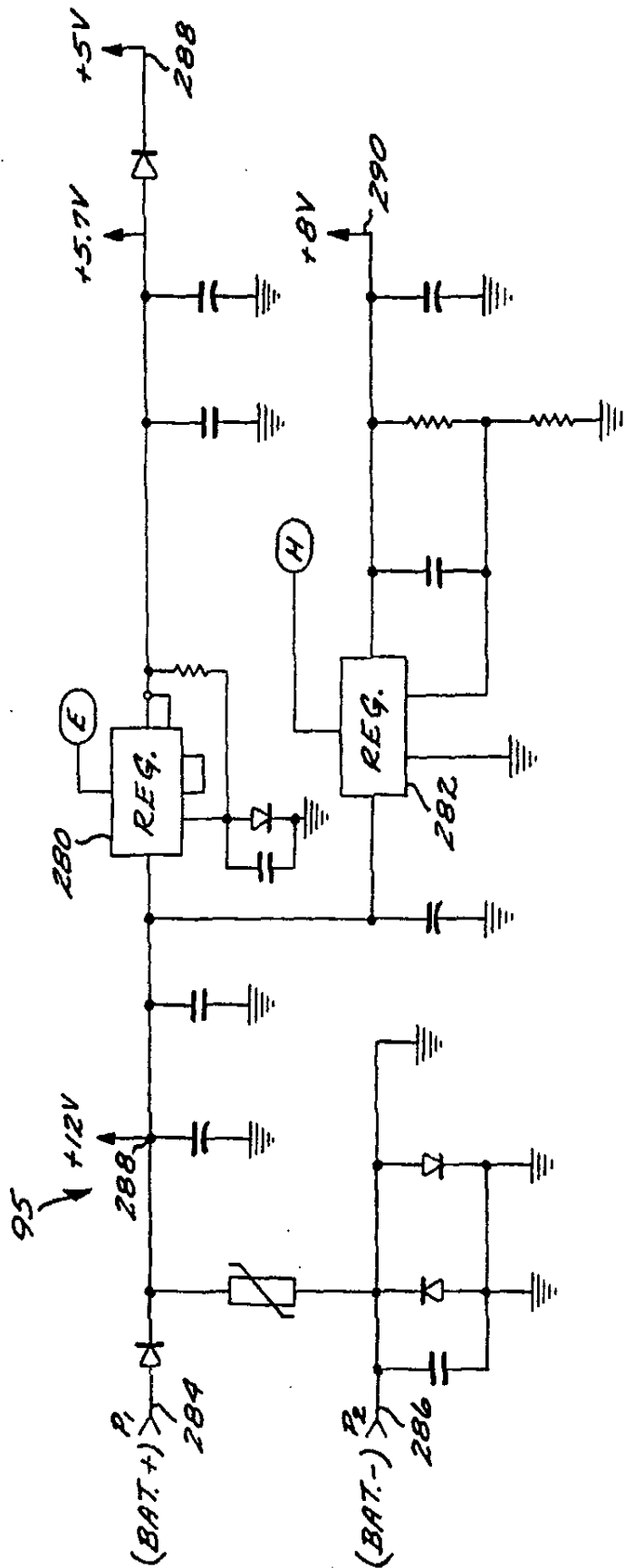


FIG. 7

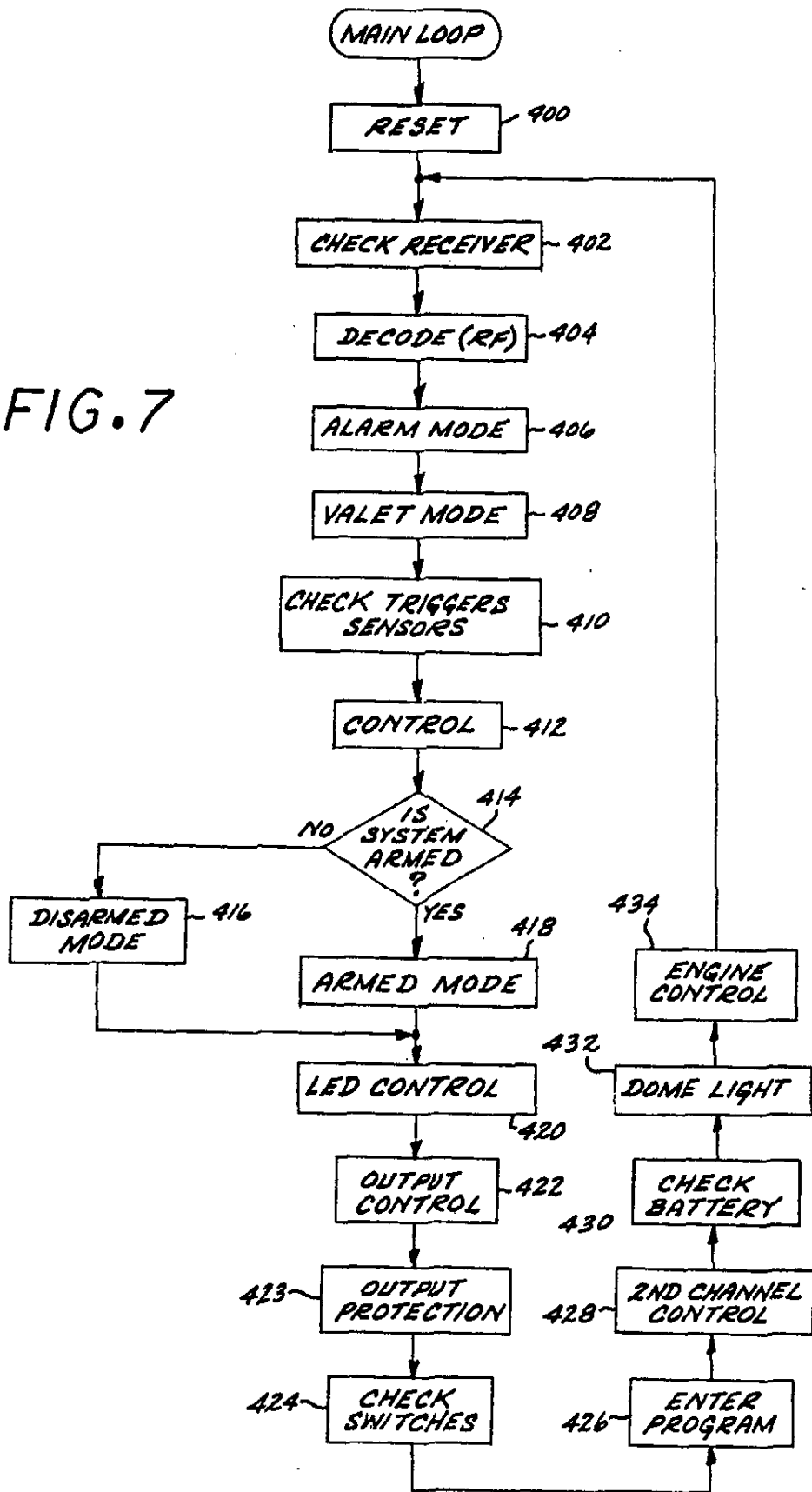


FIG. 8

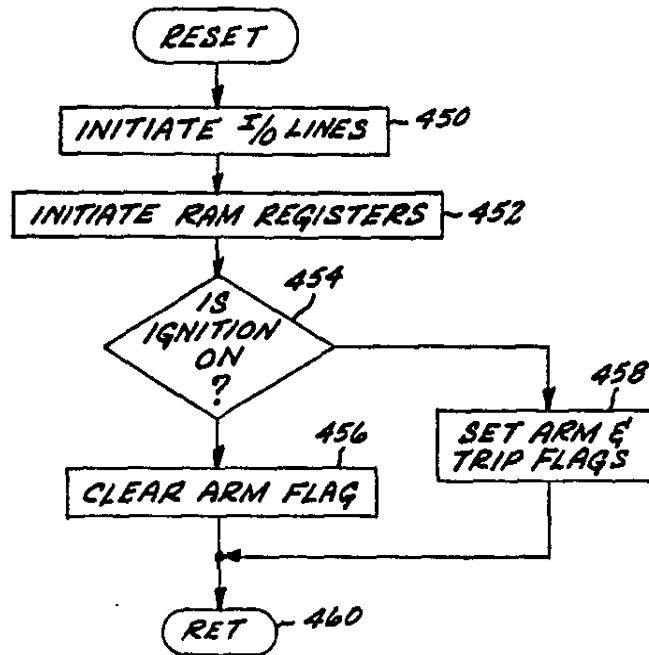
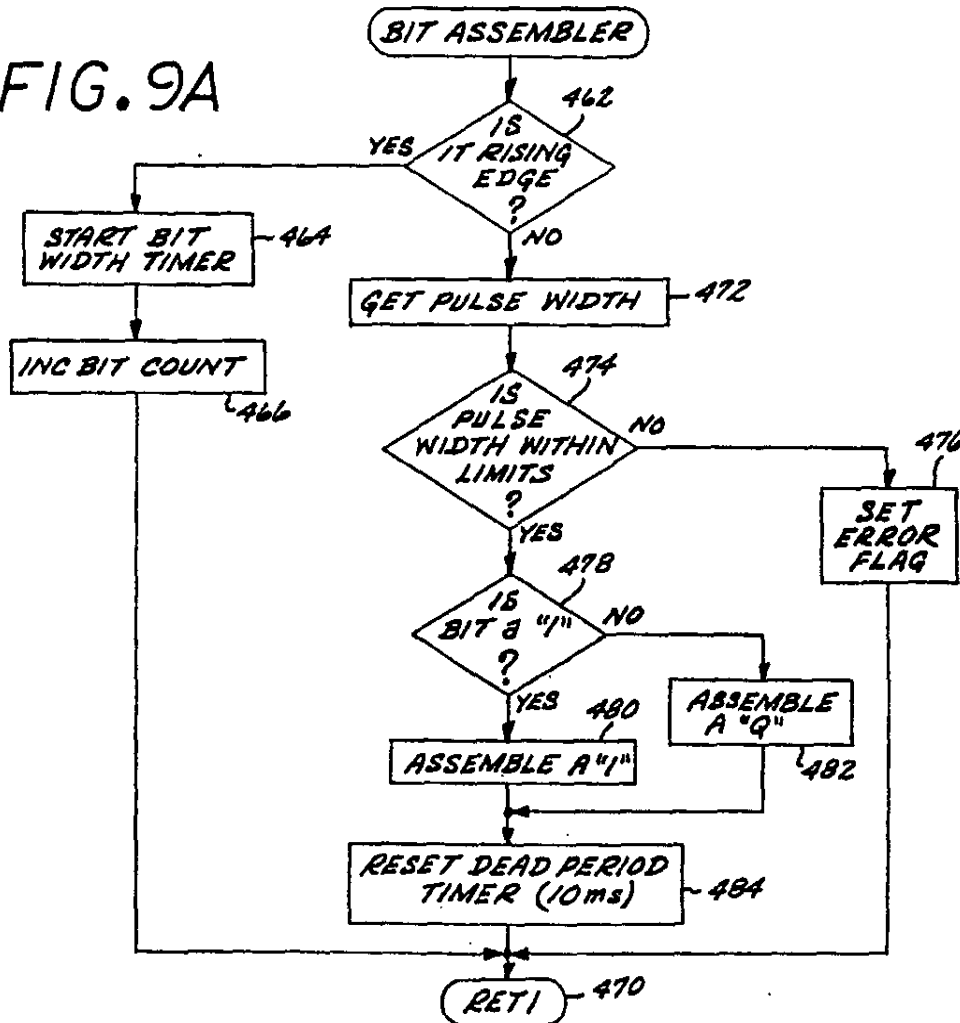


FIG. 9A



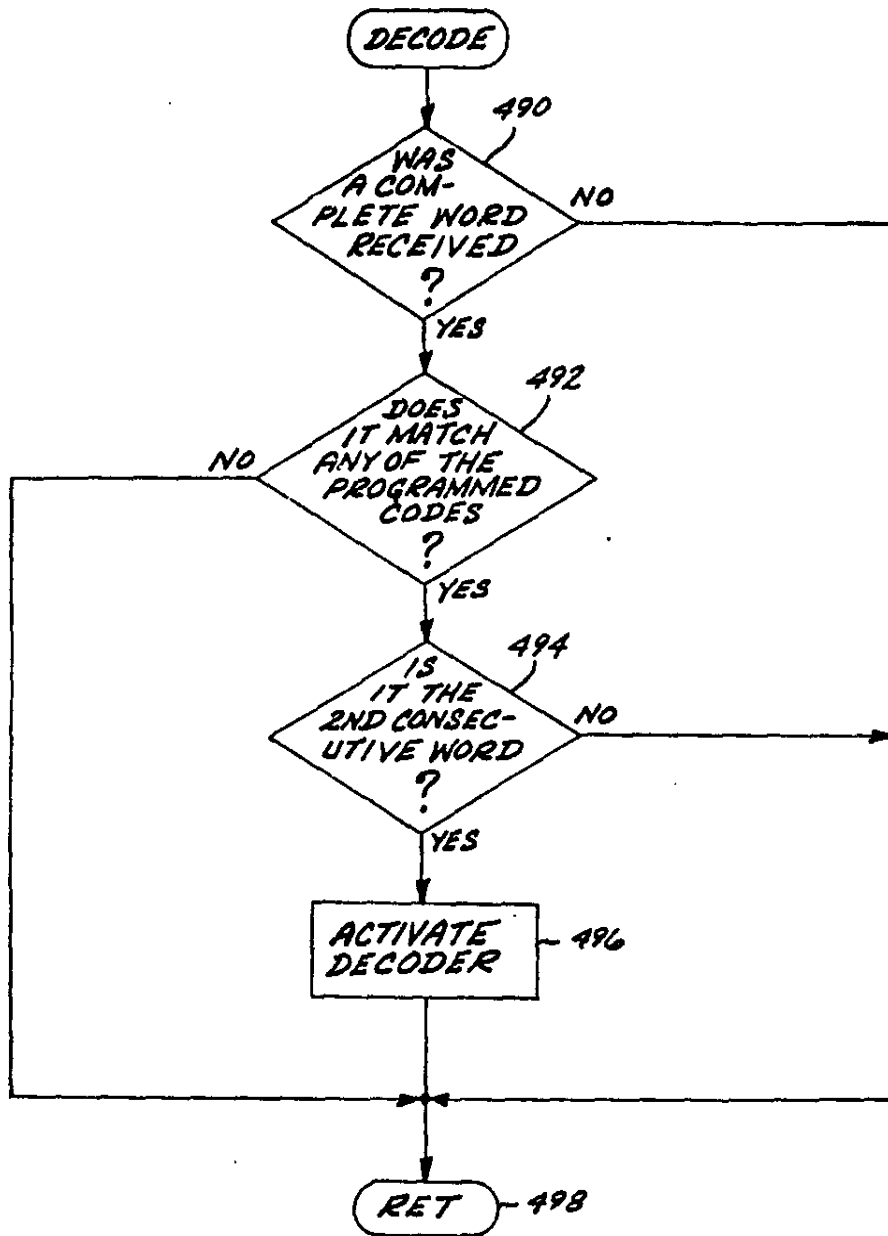


FIG. 9B

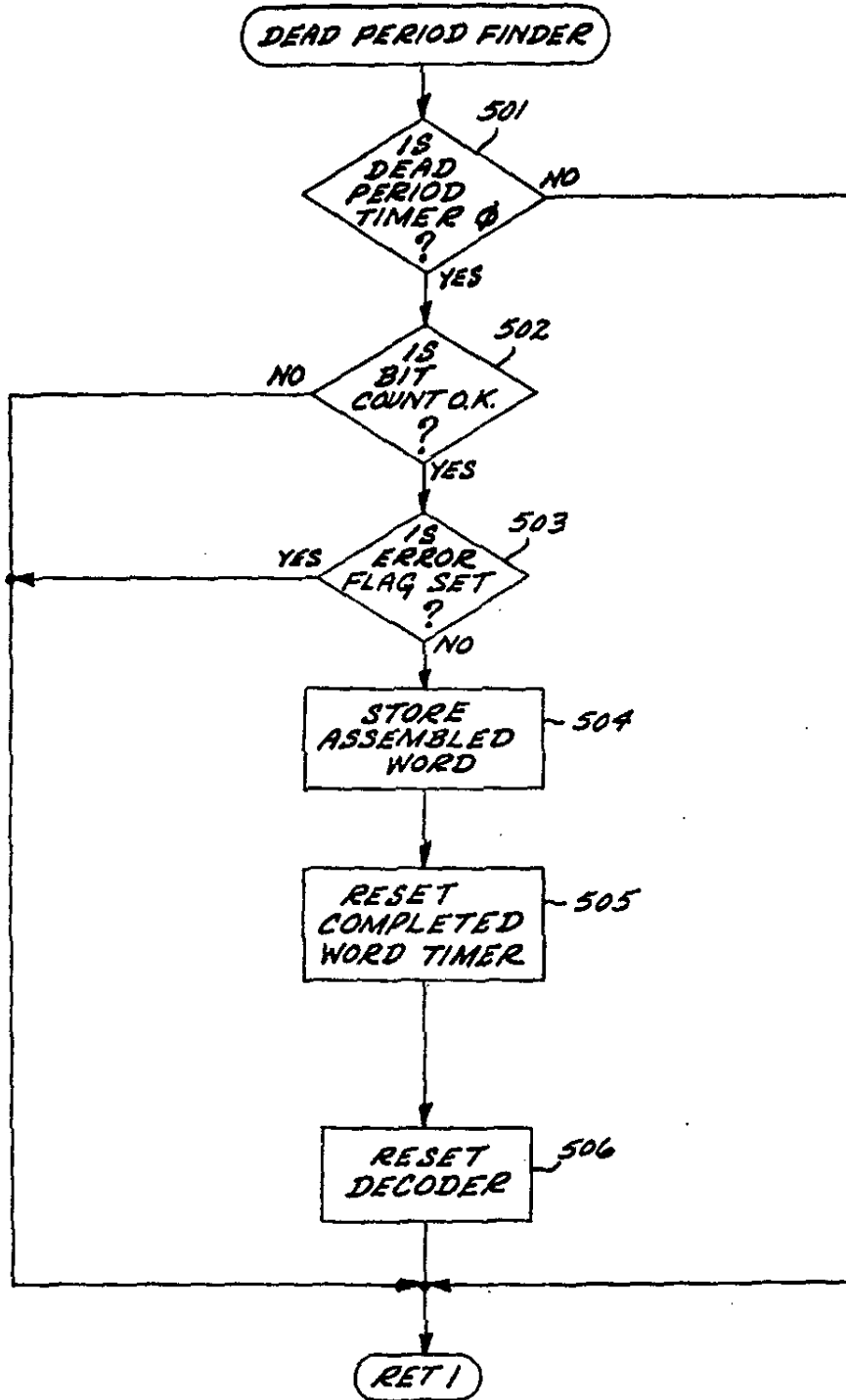


FIG. 9C

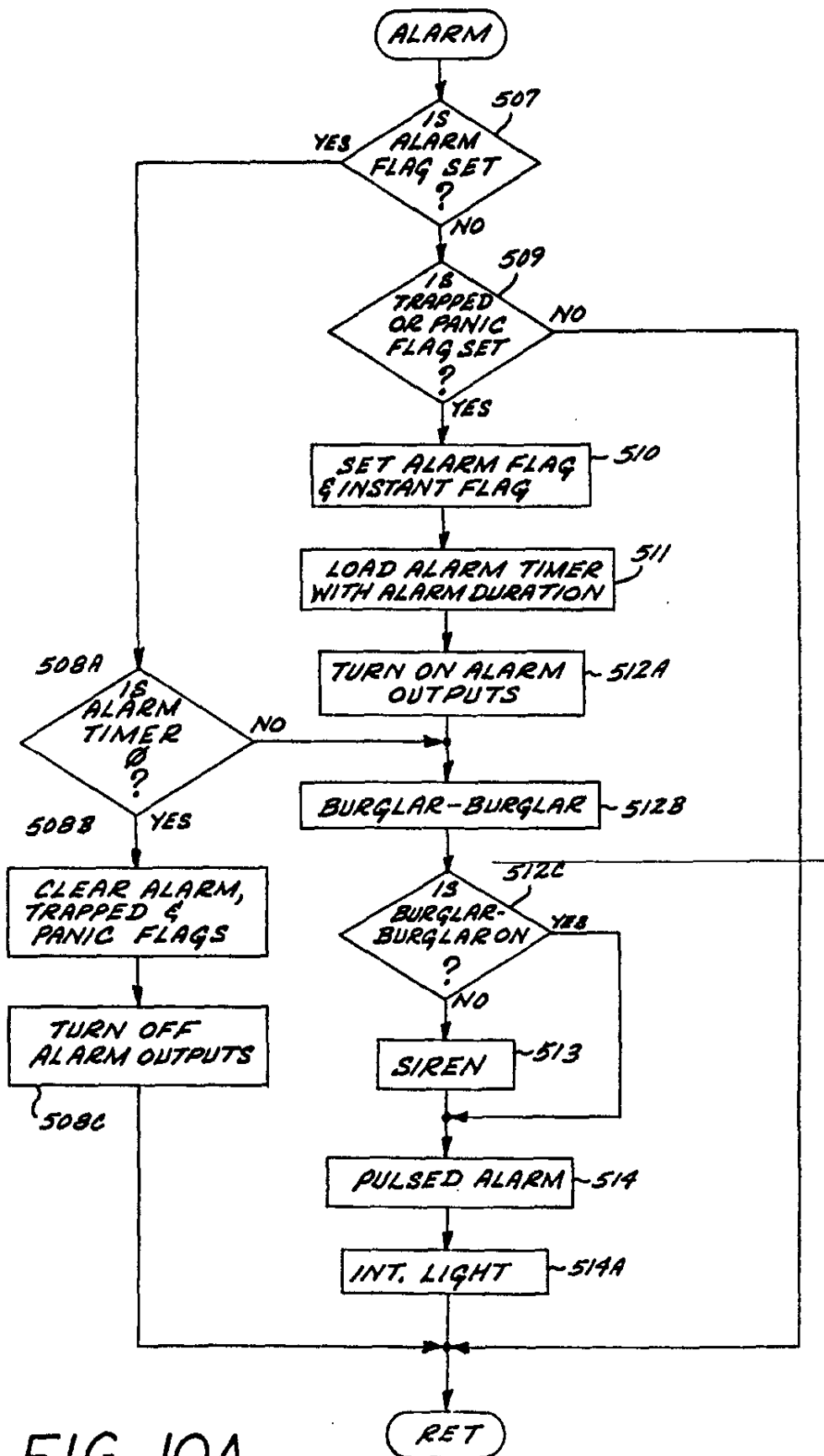


FIG. 10A

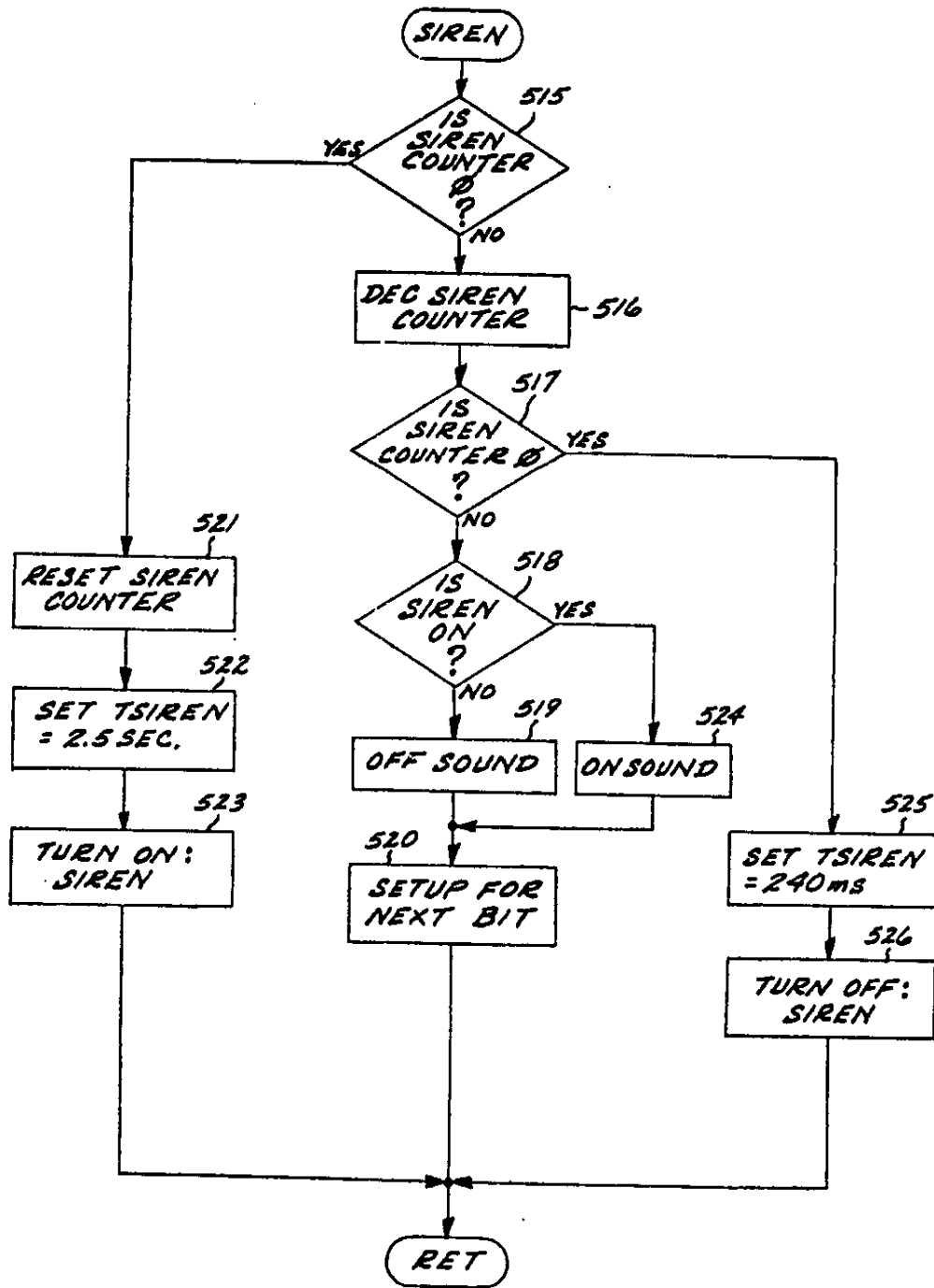


FIG. 10B

FIG. 10C

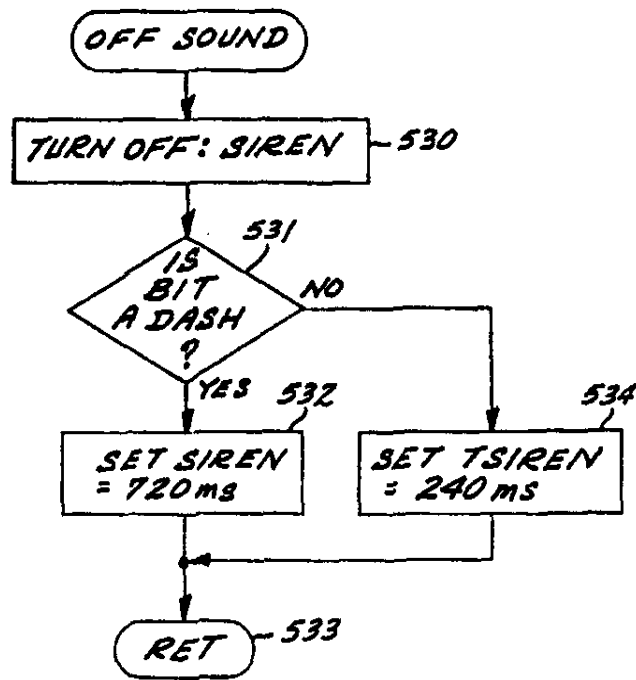


FIG. 10D

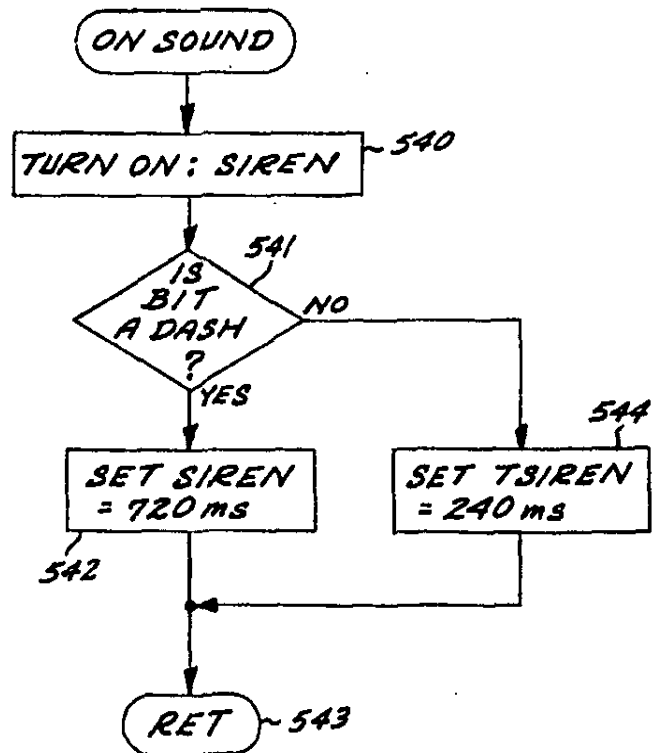


FIG. 10E

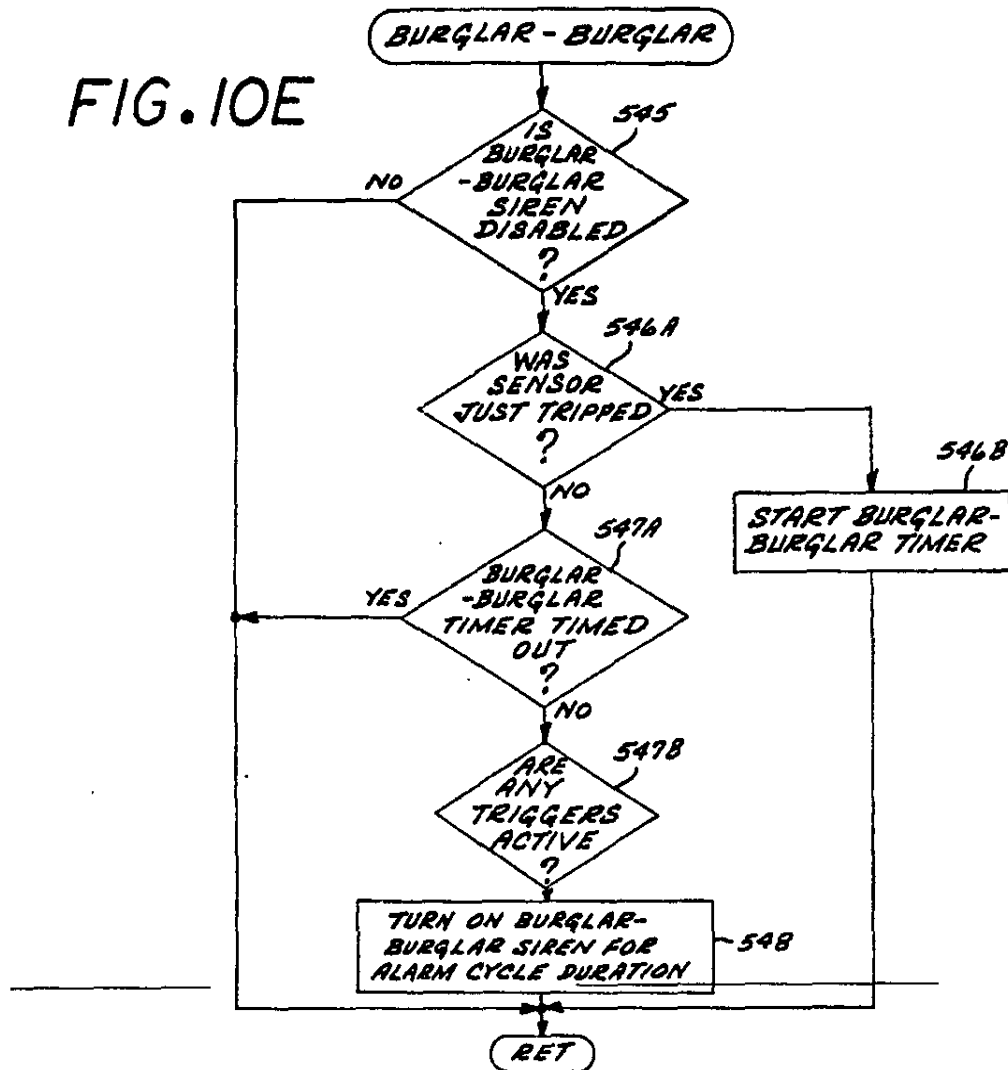
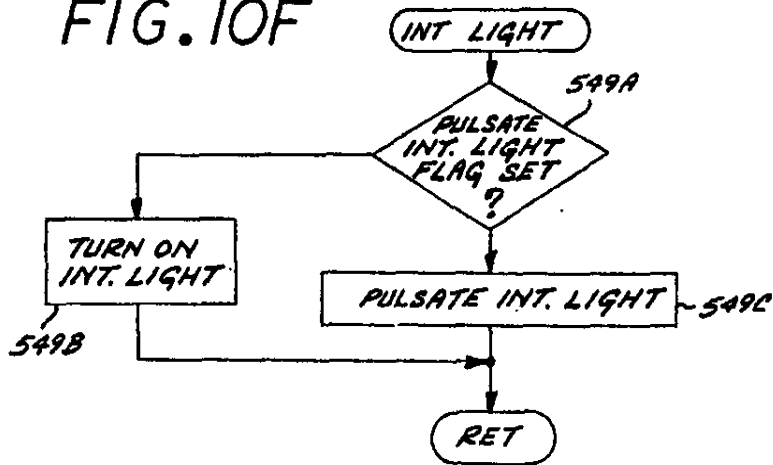


FIG. 10F



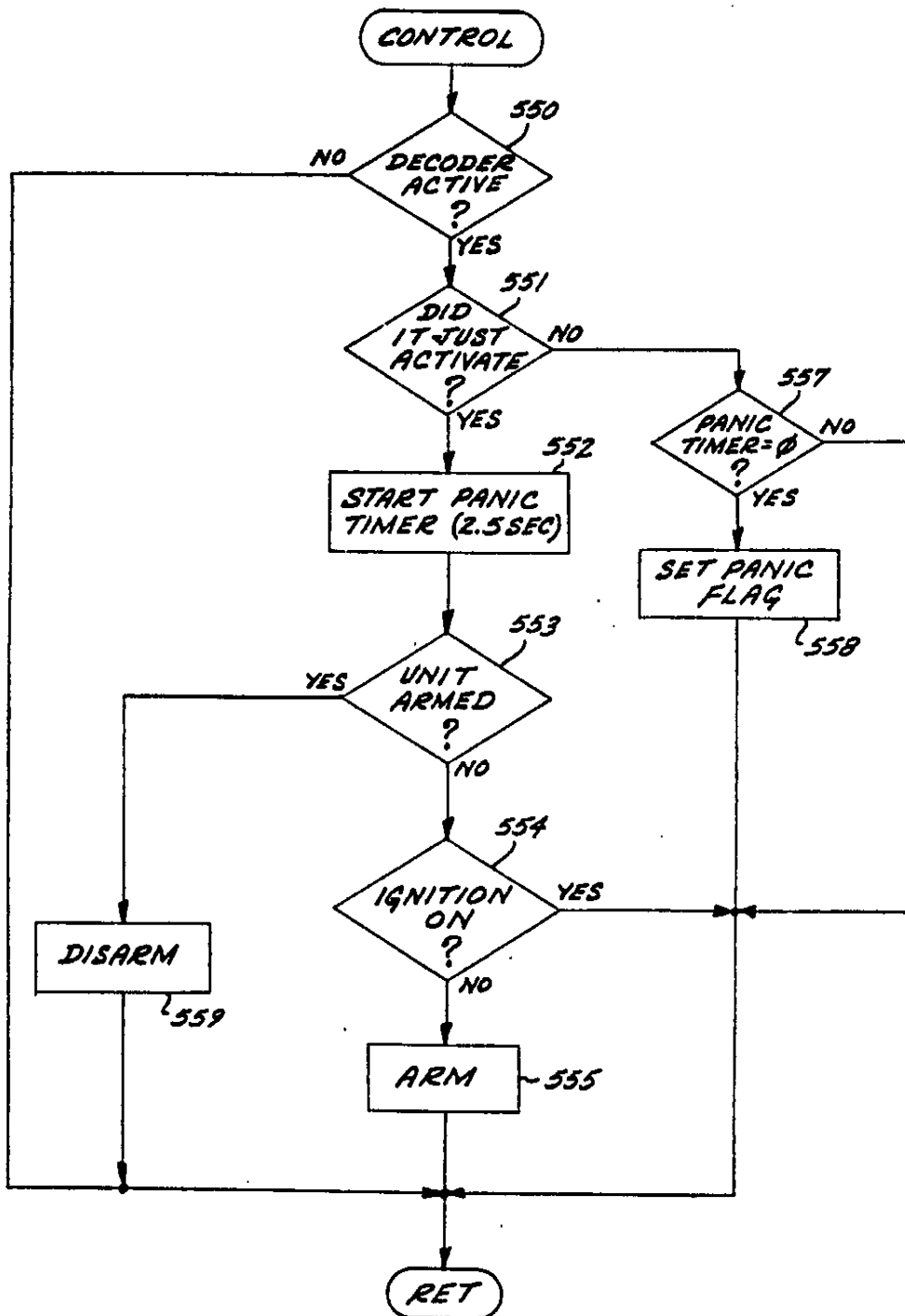


FIG. 11A

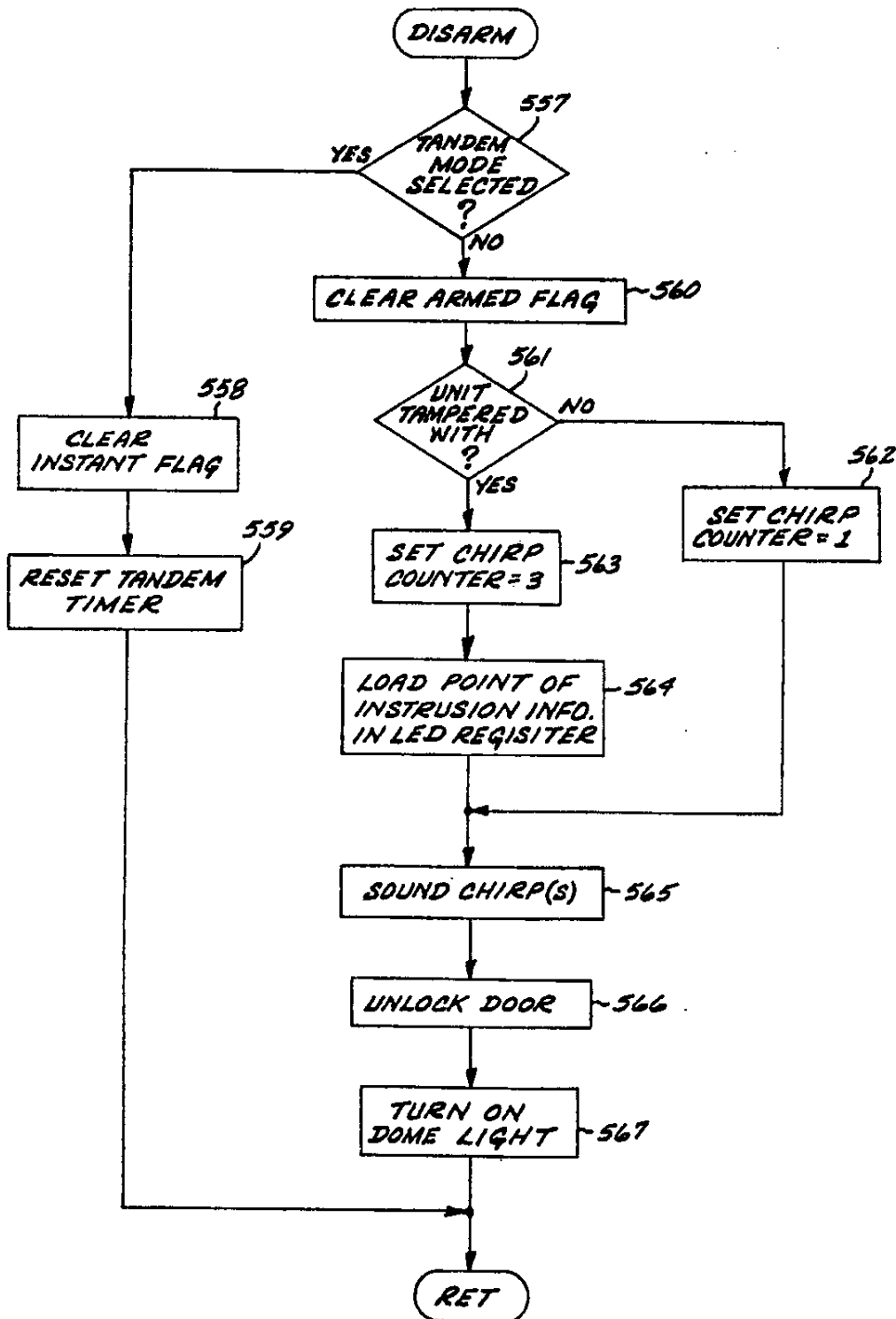


FIG. 11B

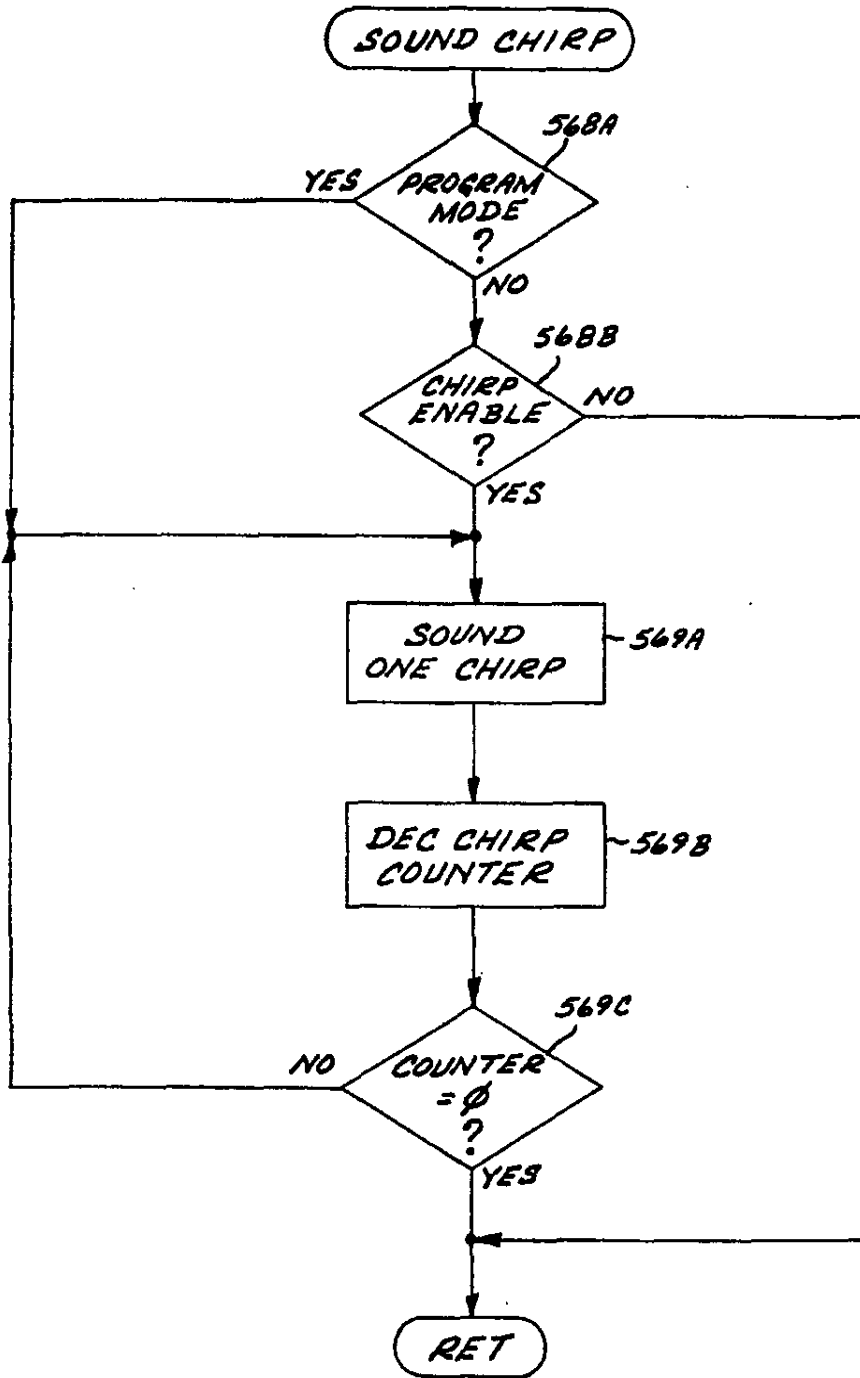


FIG. 11C

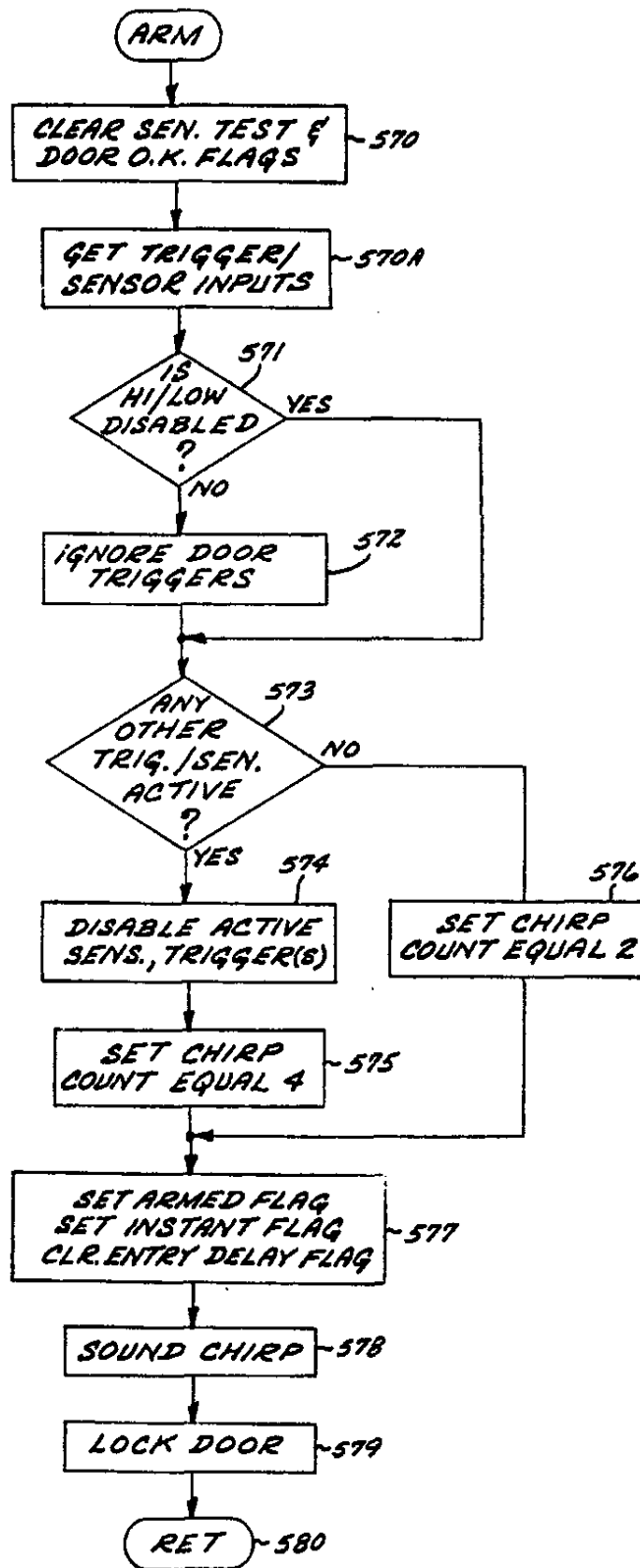
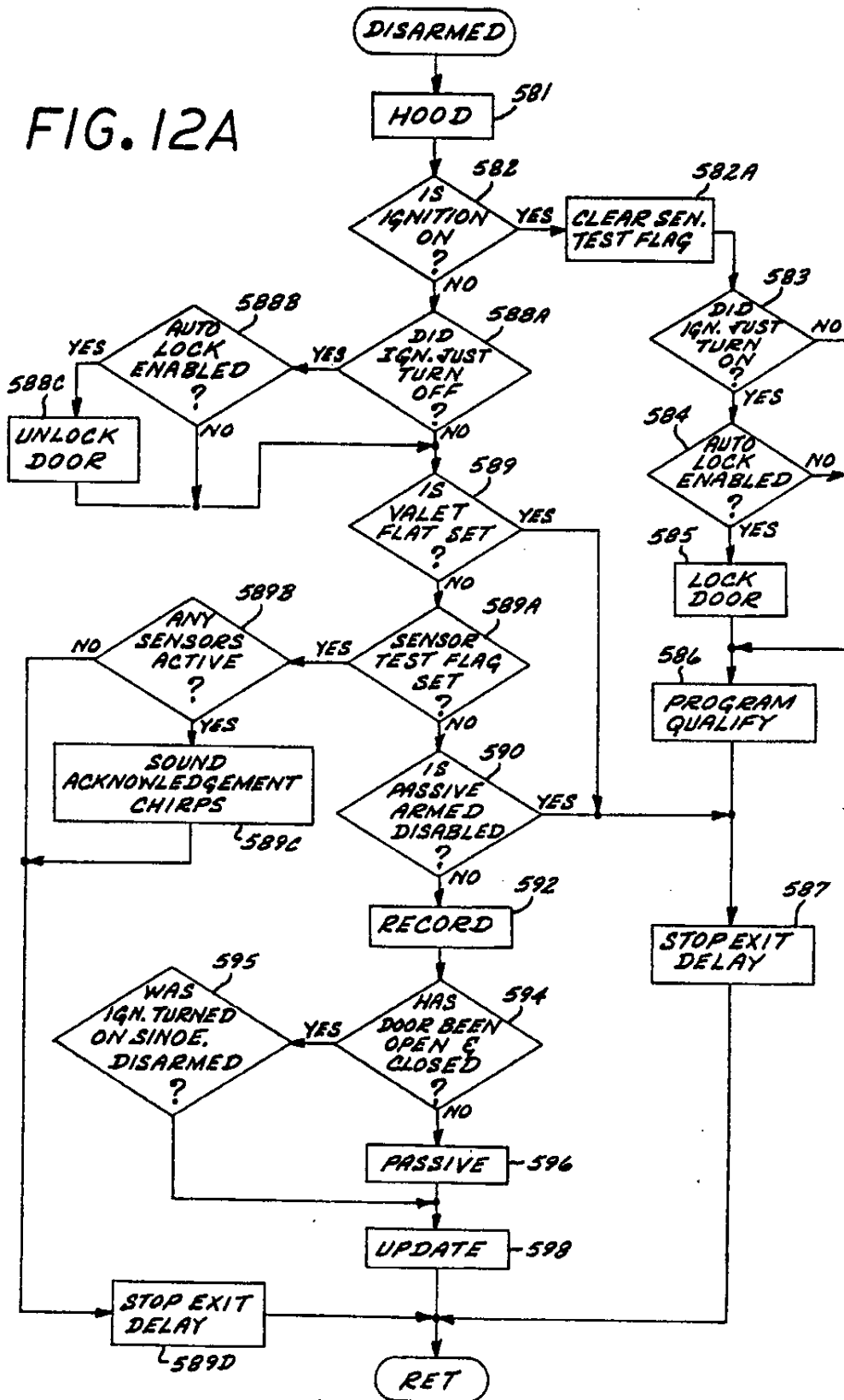


FIG. 11D

FIG. 12A



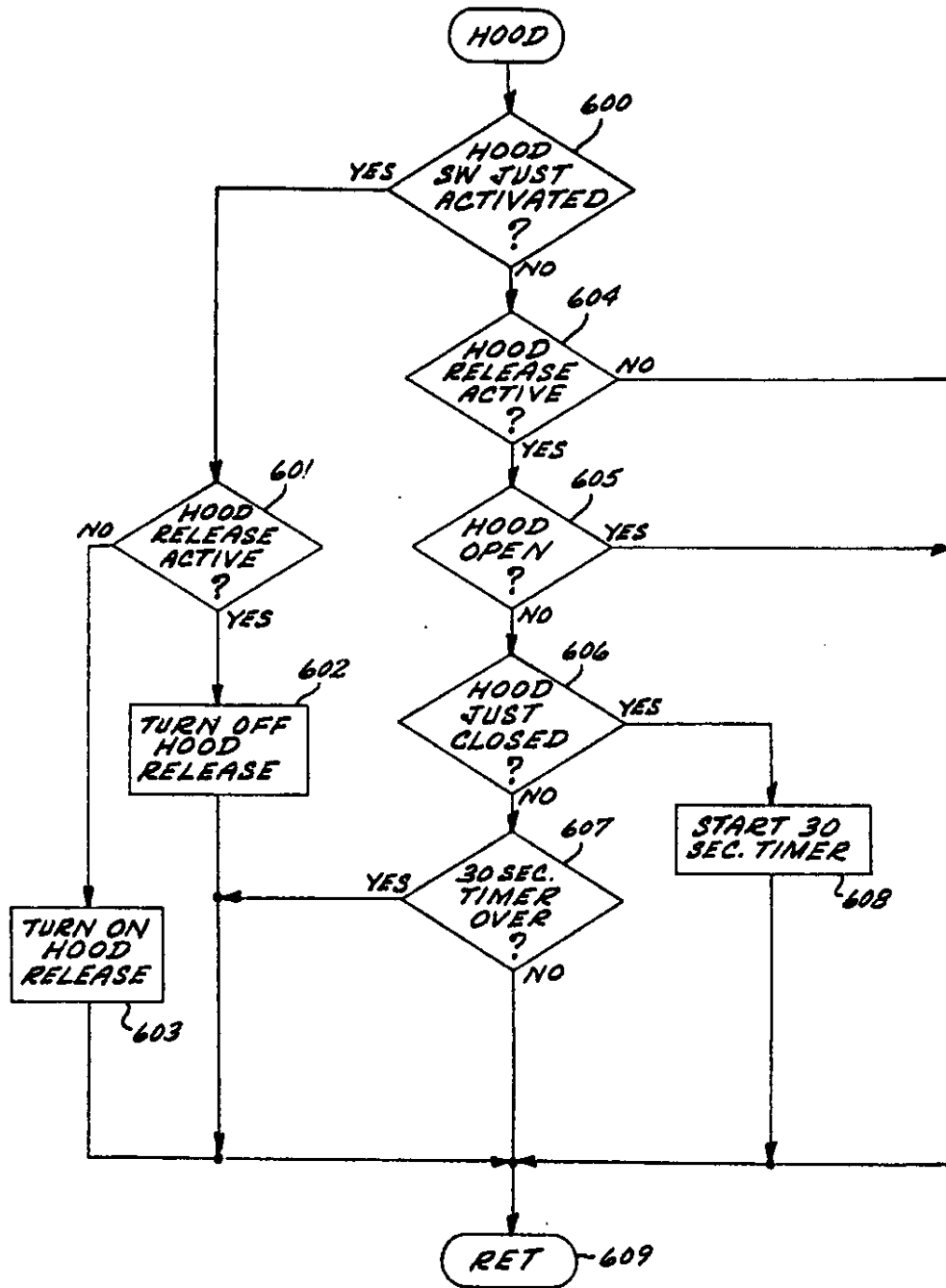
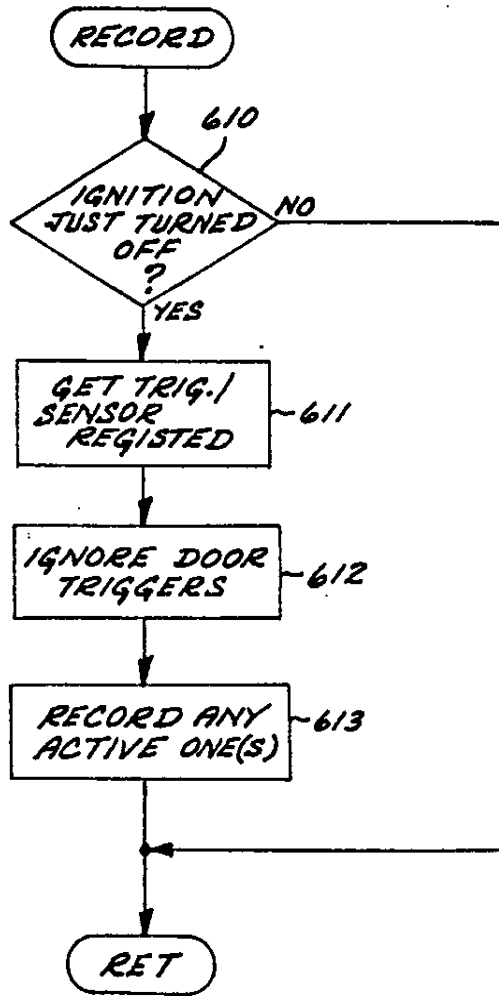


FIG. 12B

FIG. 12C



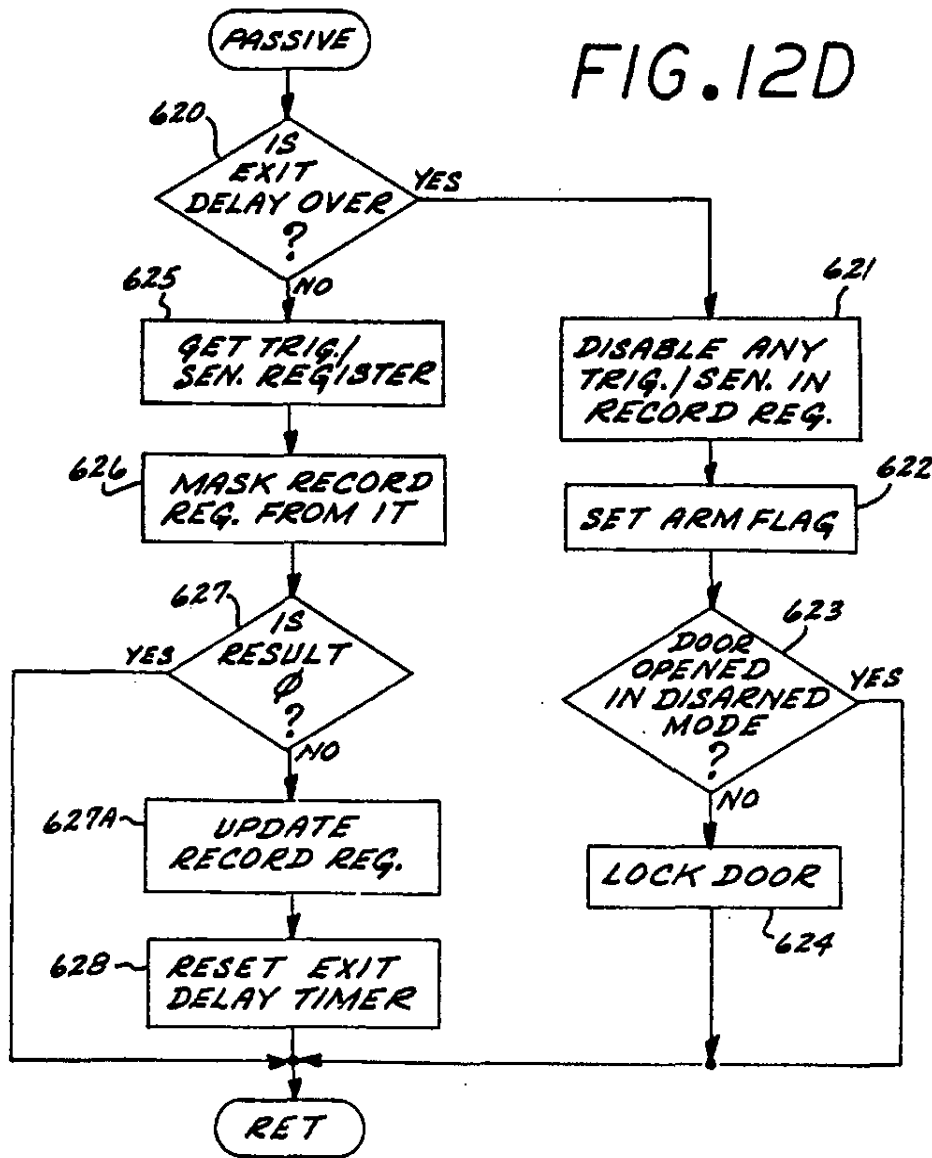
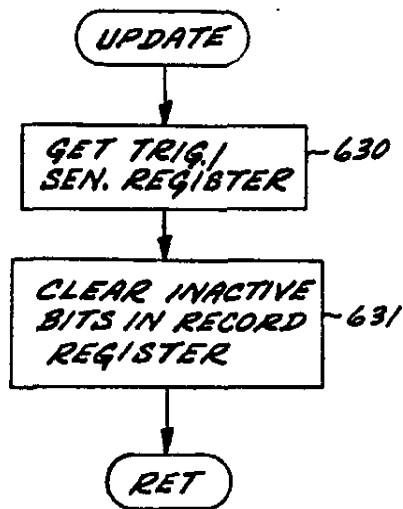


FIG. 12E



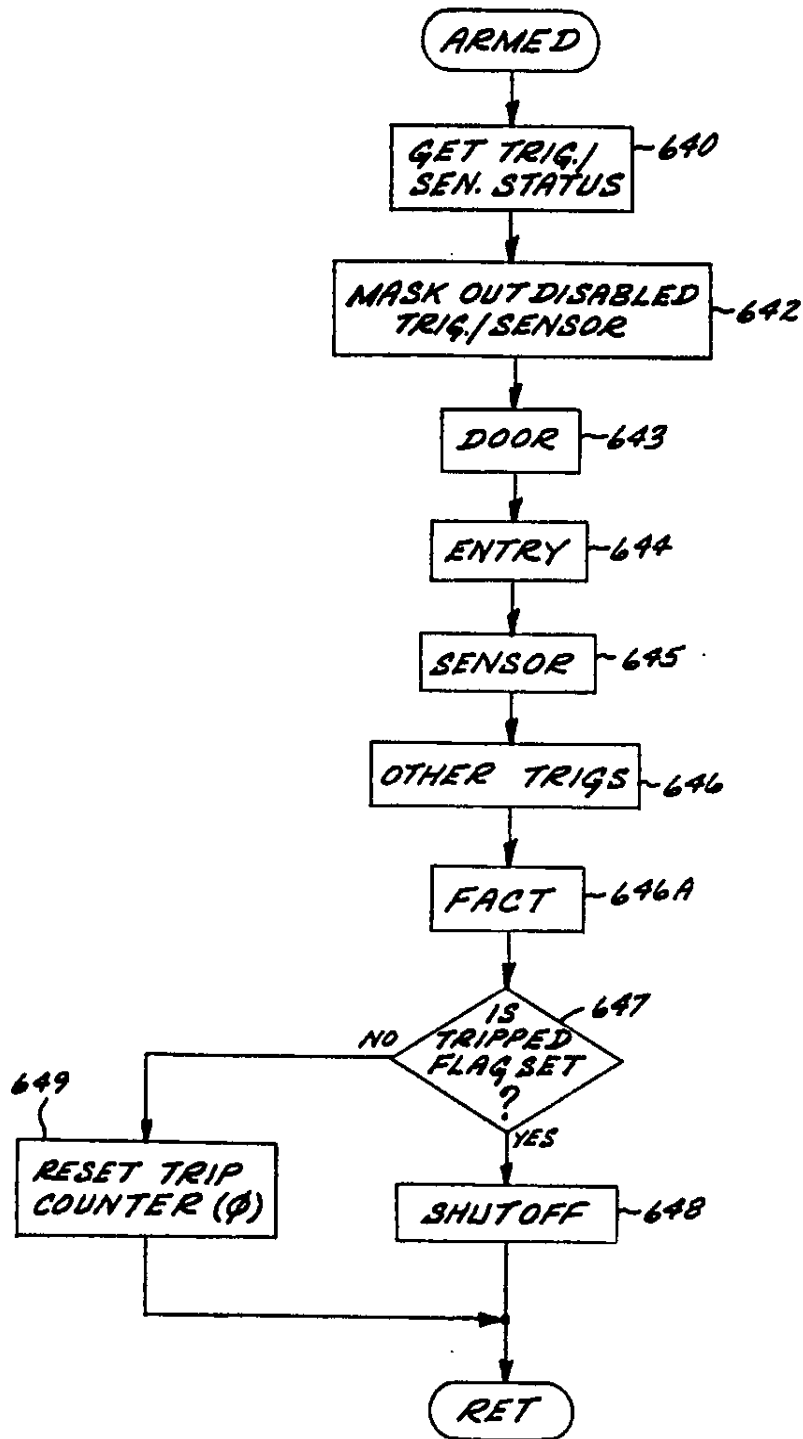


FIG. 13A

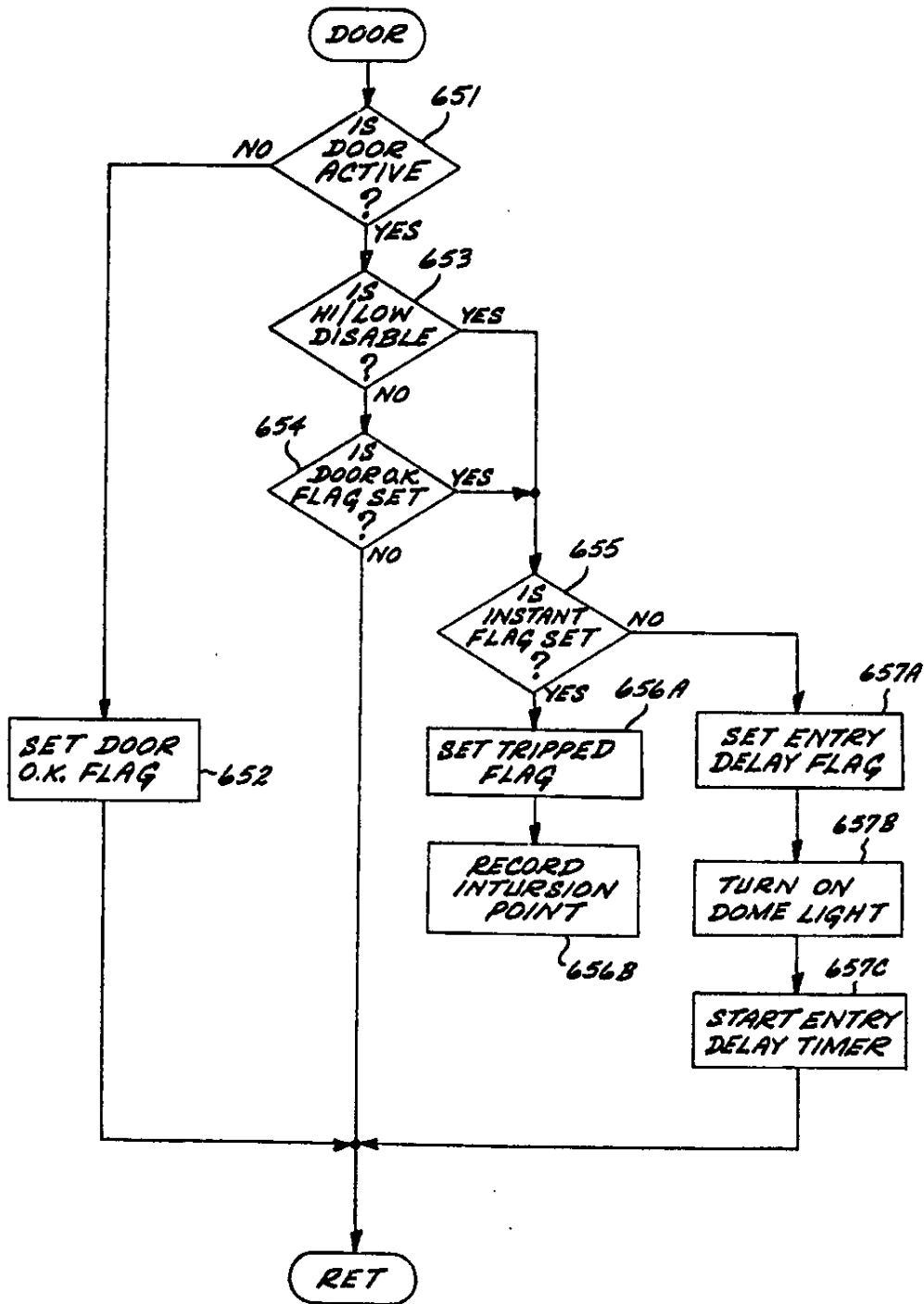


FIG. 13B

FIG. 13C

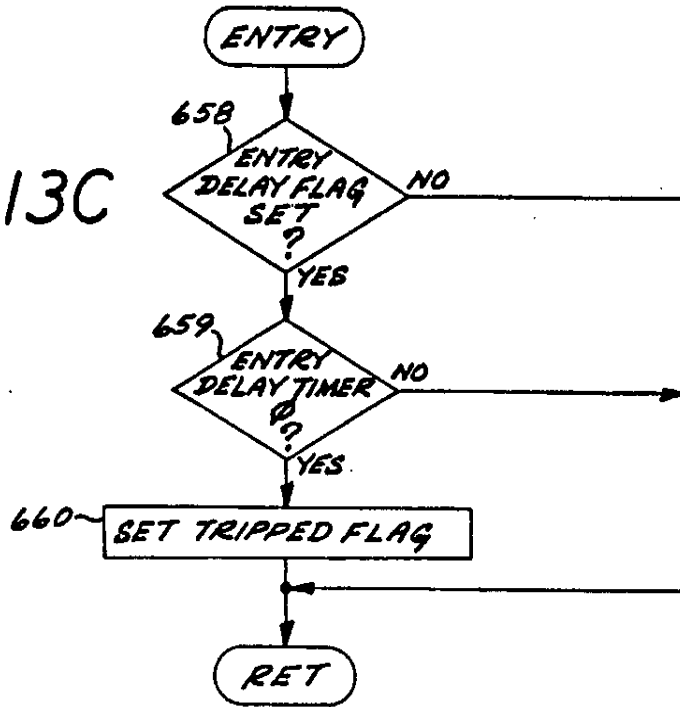


FIG. 13D

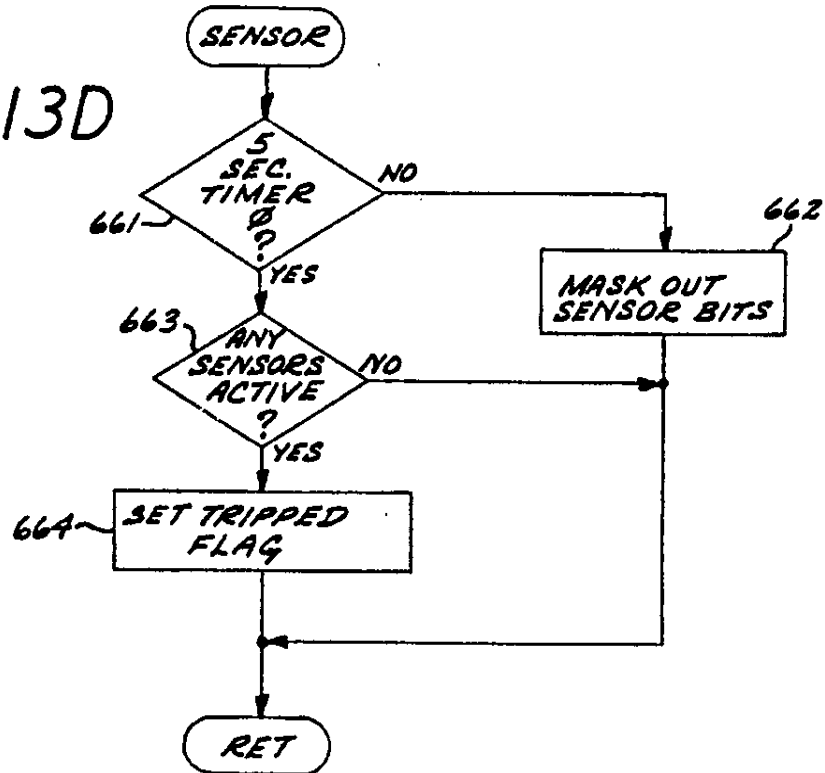


FIG. 13E

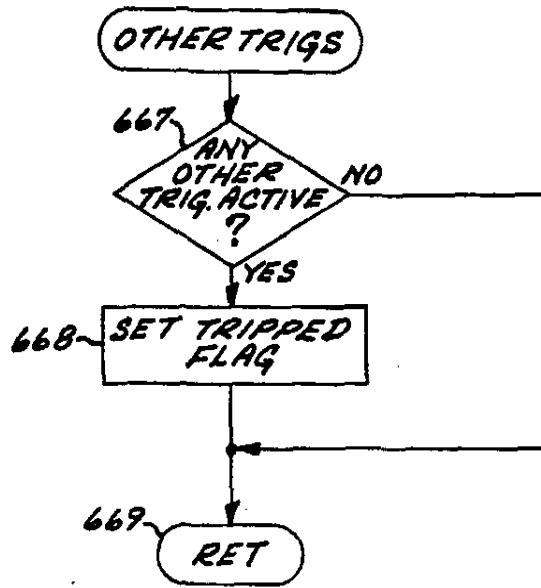


FIG. 13F

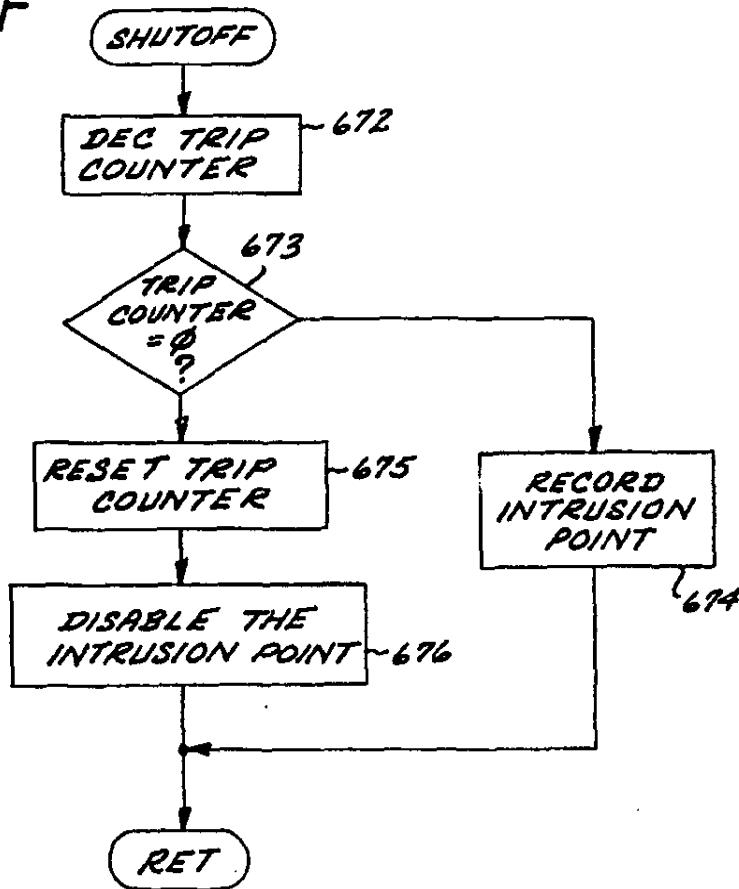


FIG. 13G

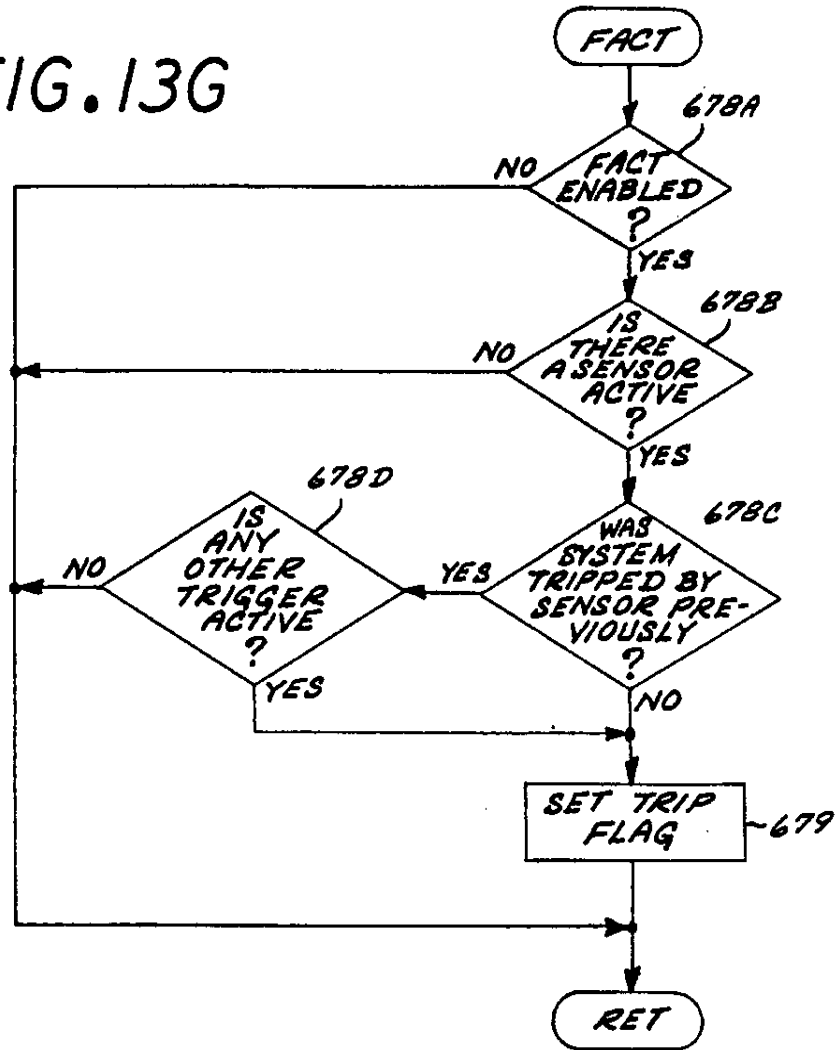
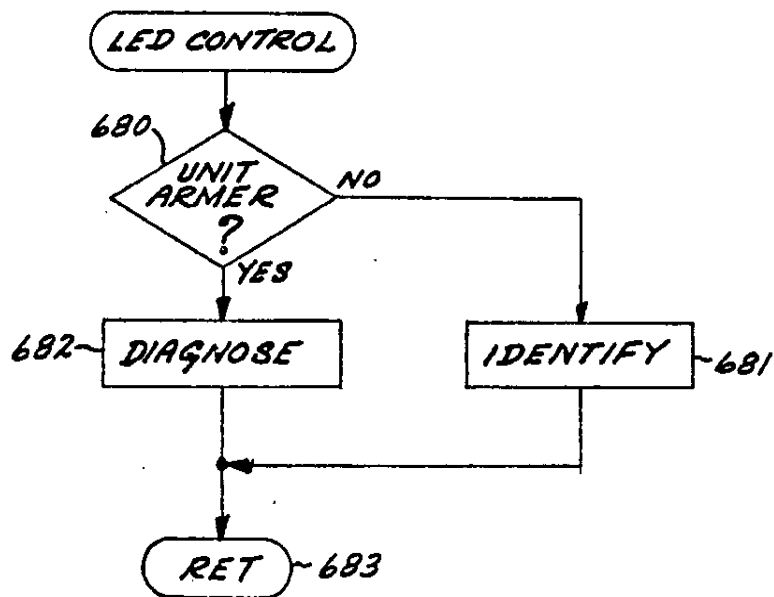


FIG. 14A



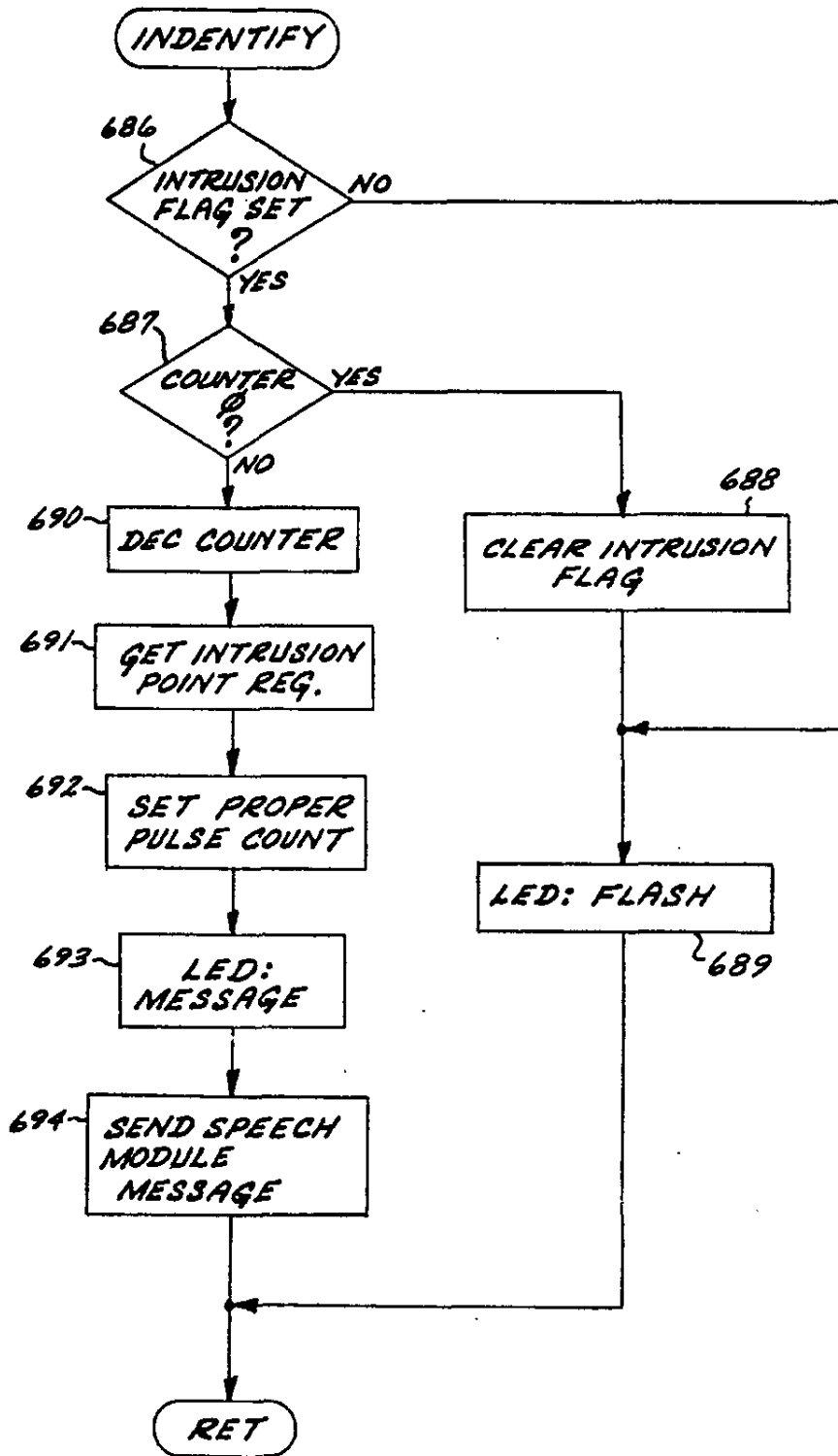


FIG. 14B

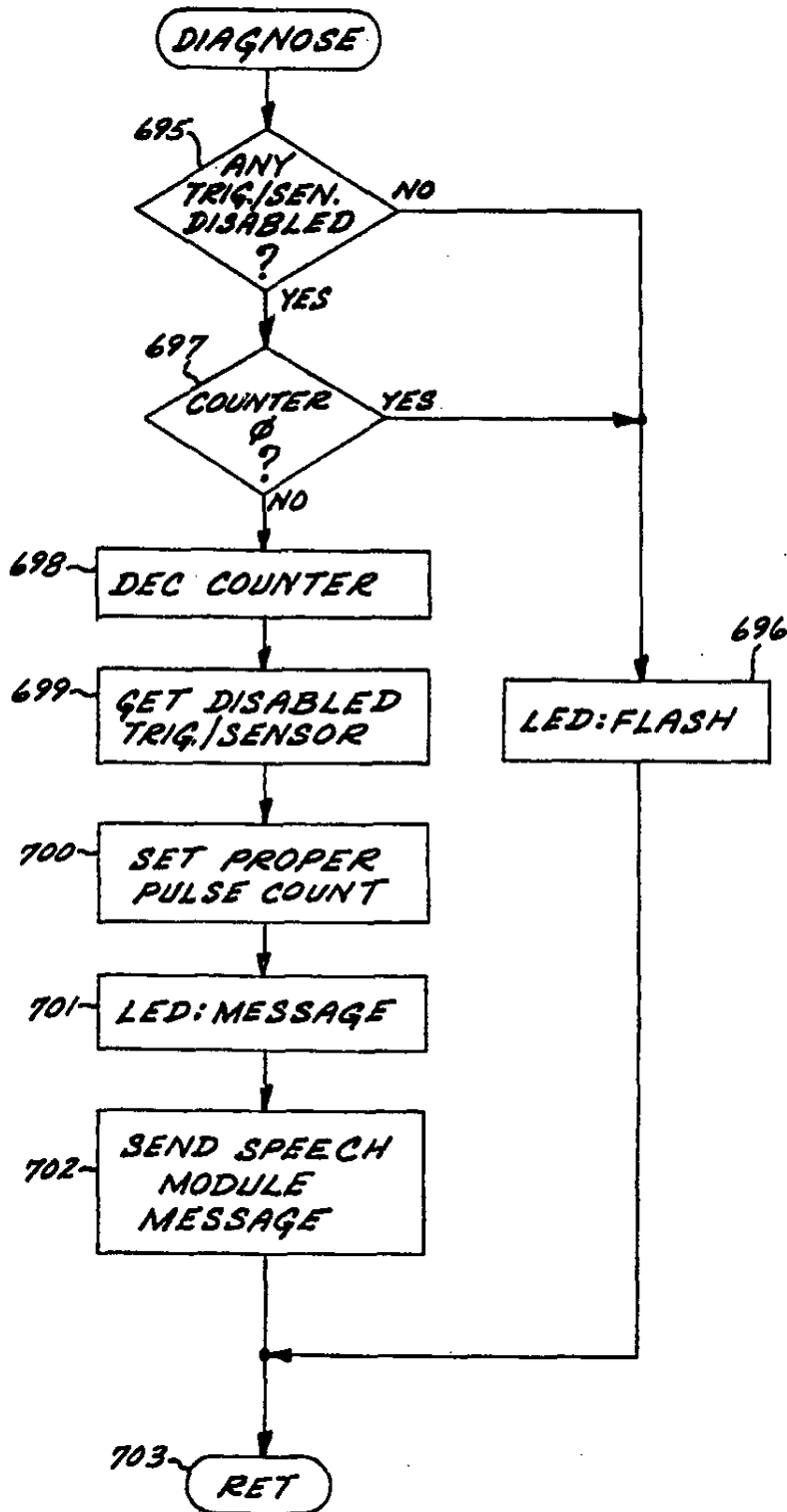


FIG. 14C

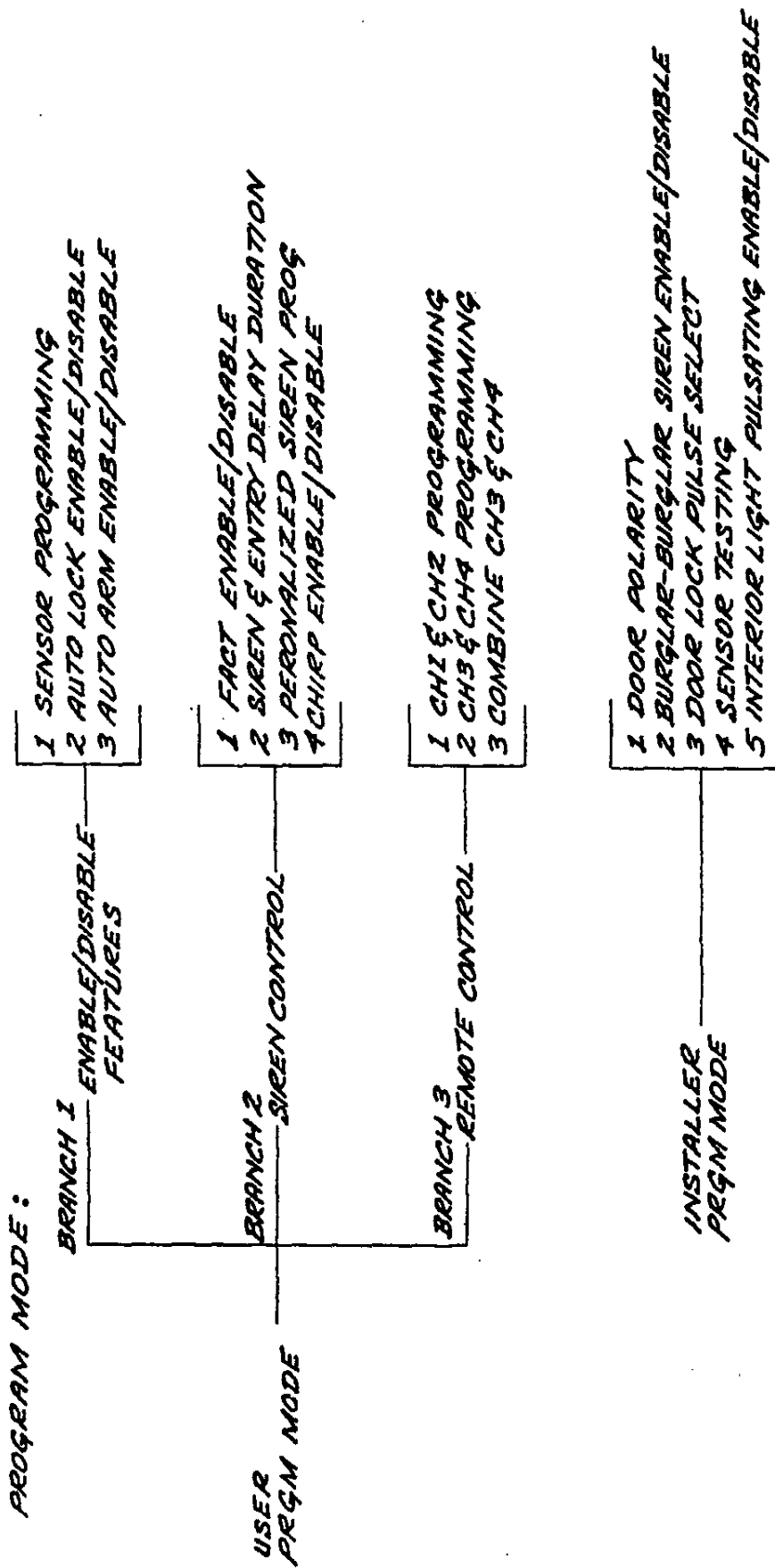


FIG. 15A

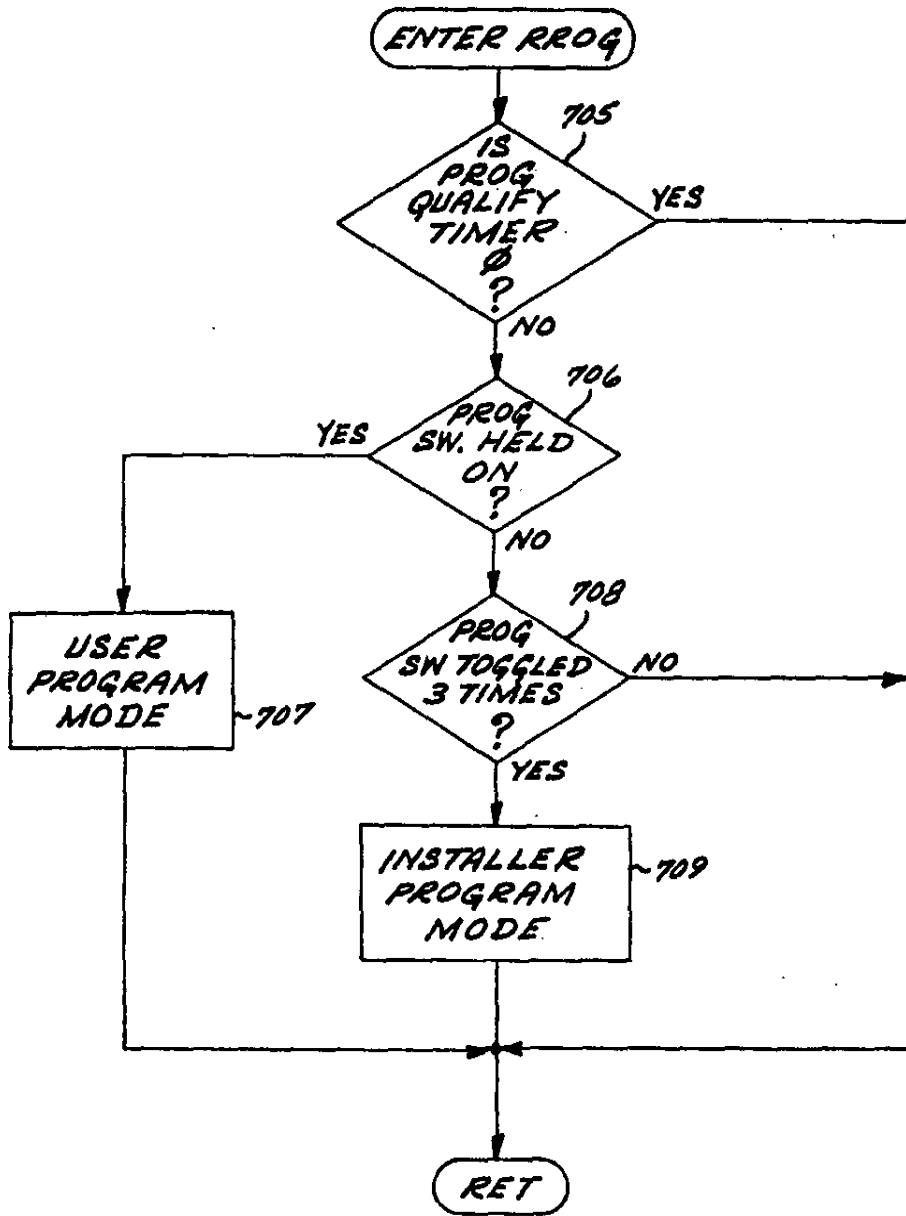


FIG. 15B

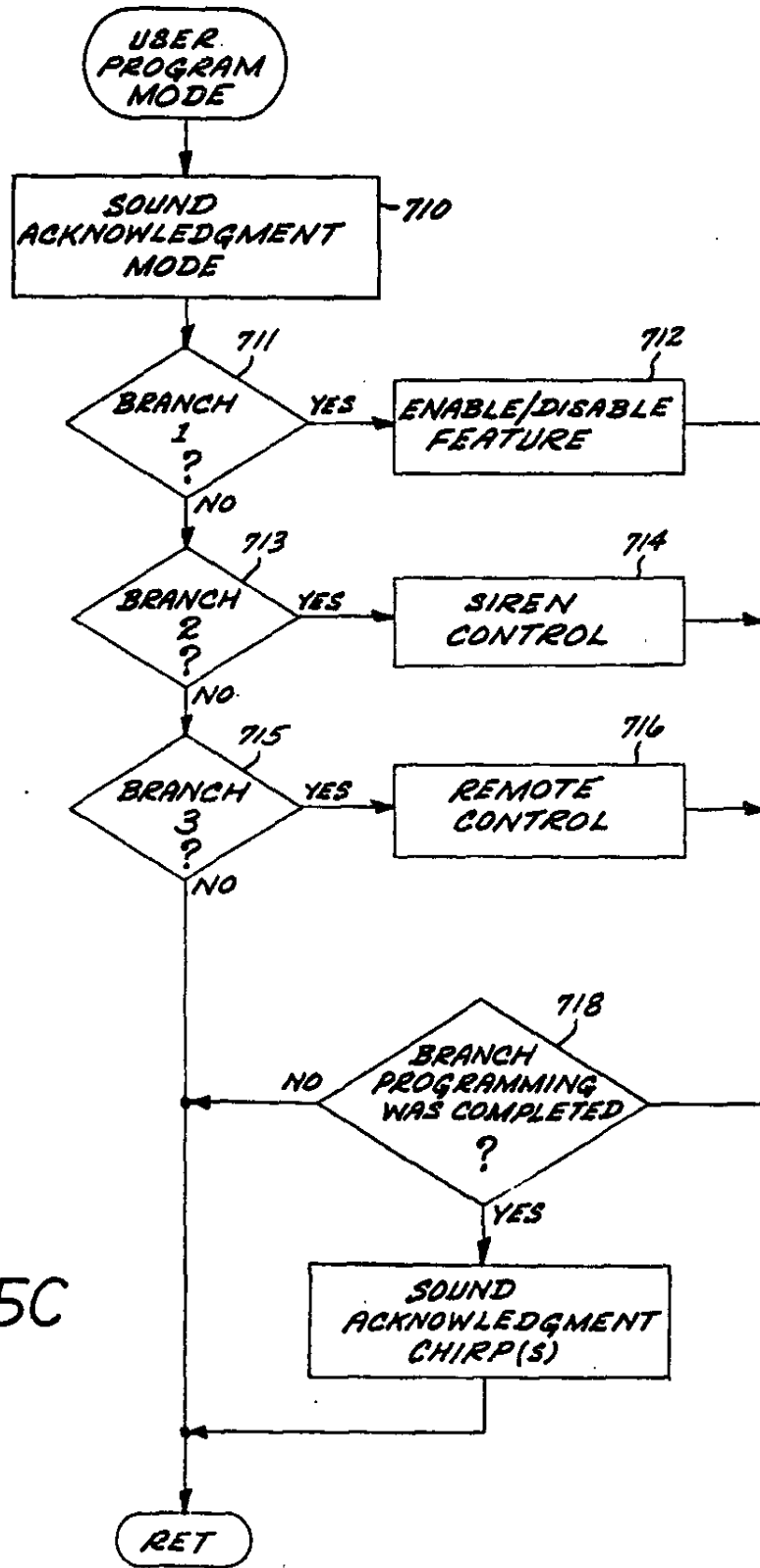


FIG. 15C

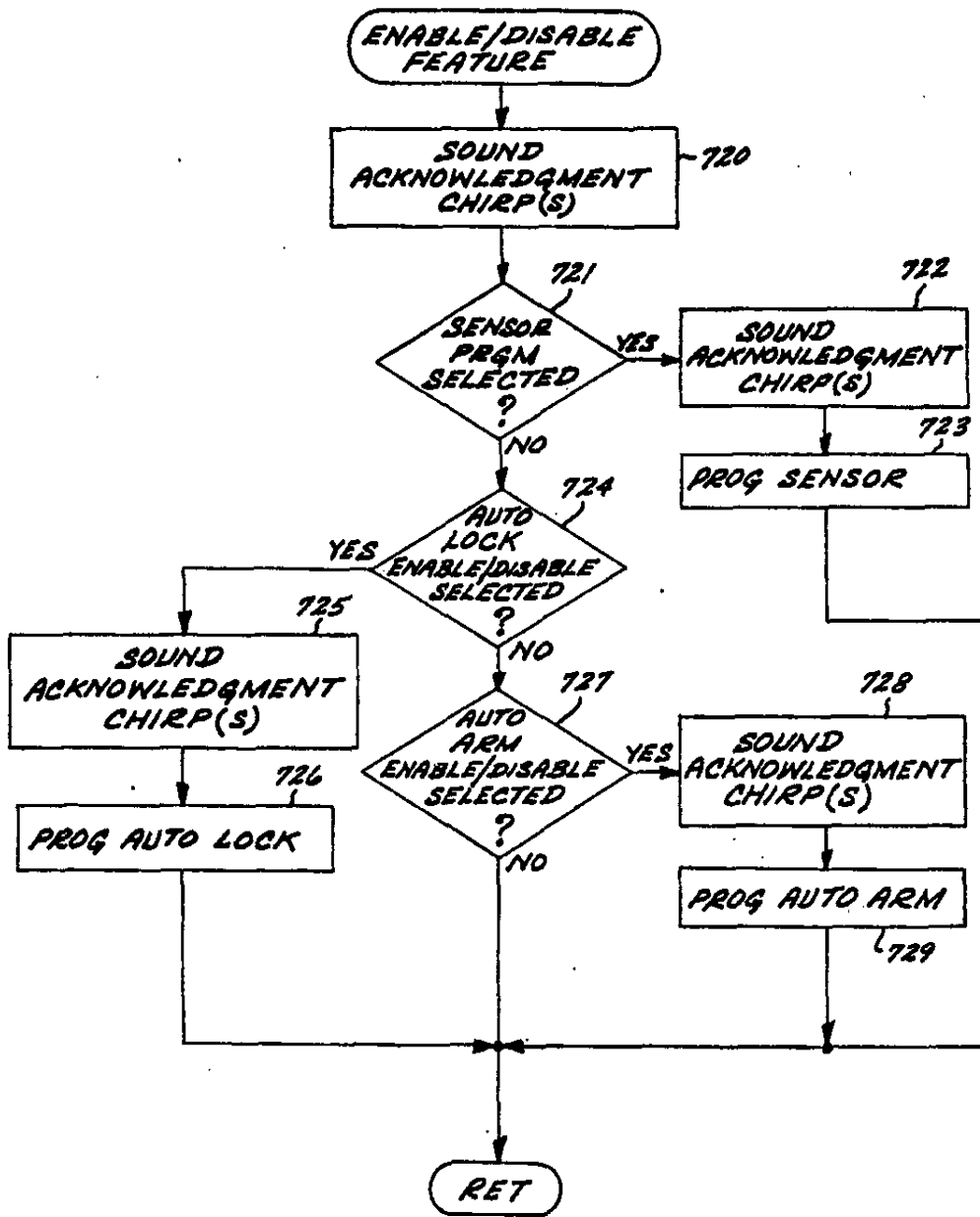


FIG. 15D

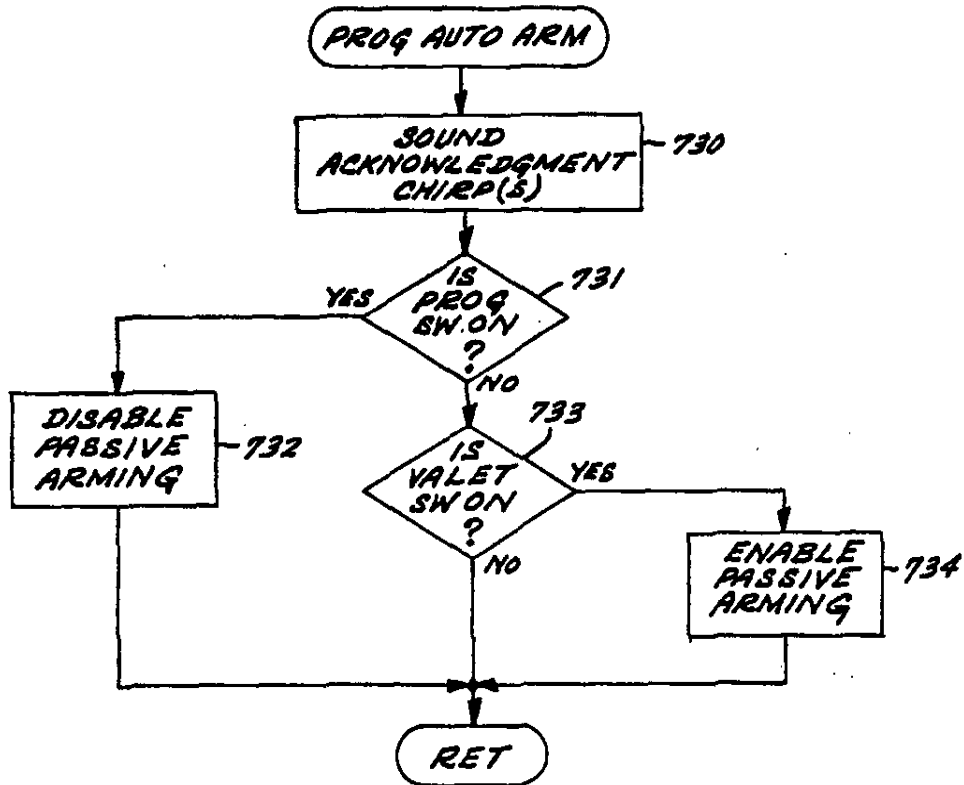


FIG. 15E

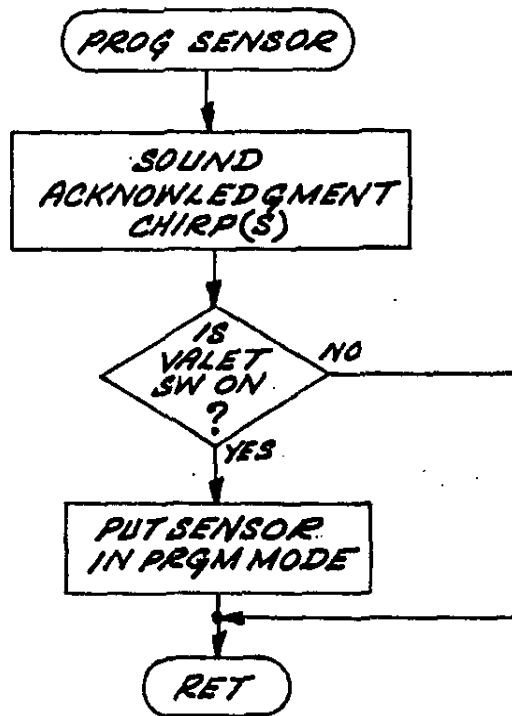


FIG. 15F

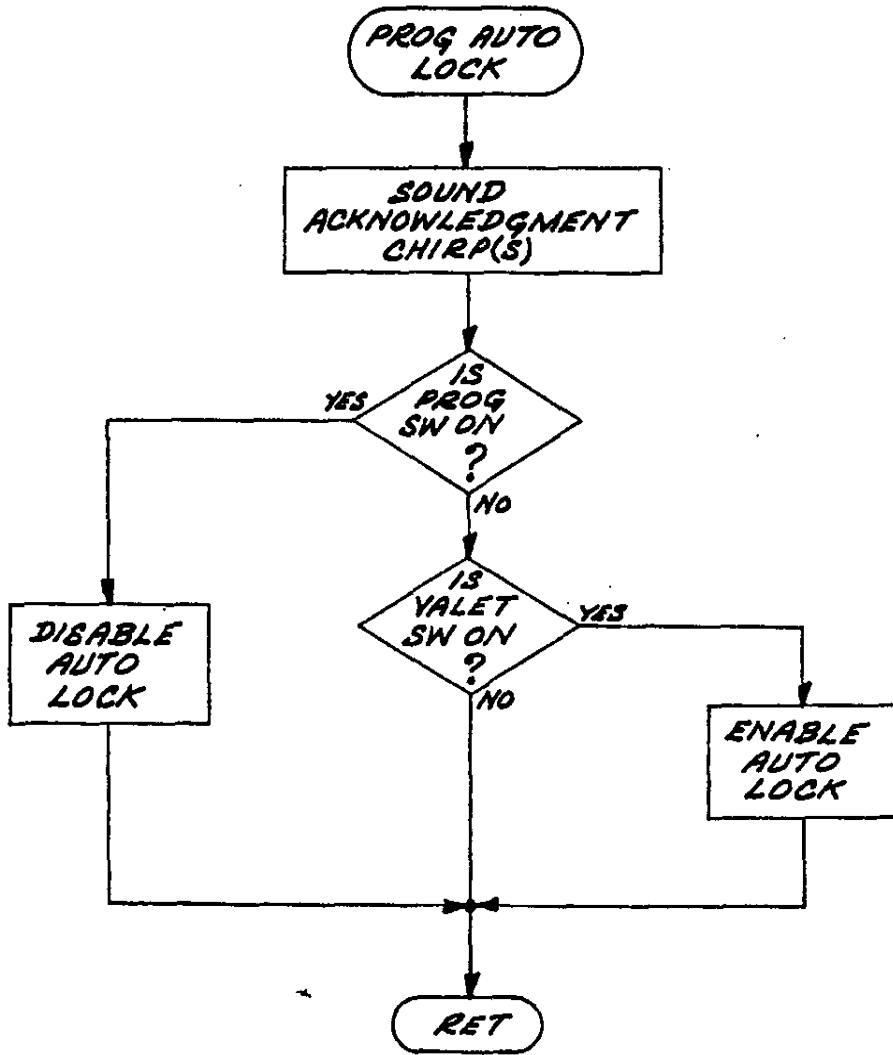


FIG. 15G

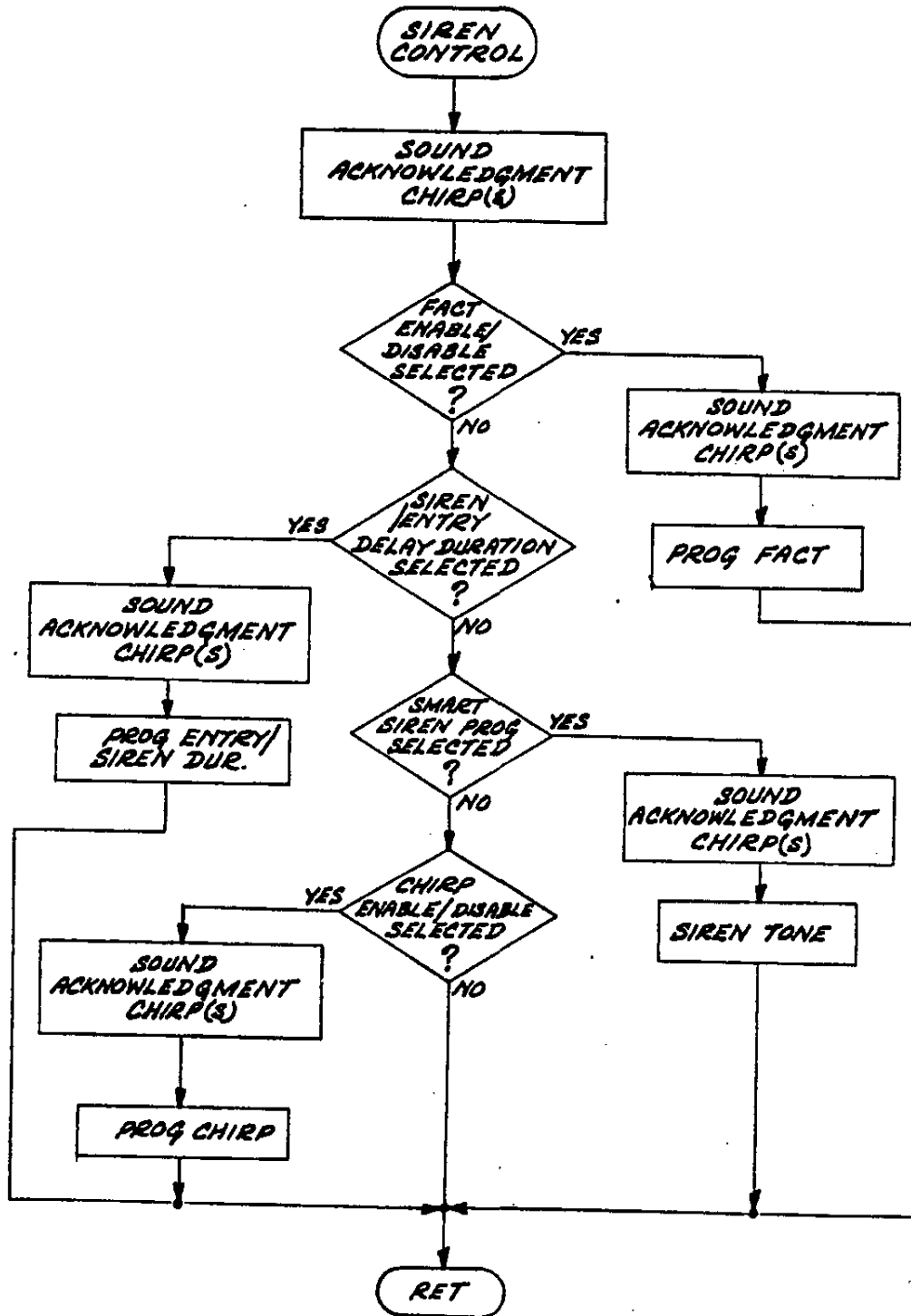


FIG. 15H

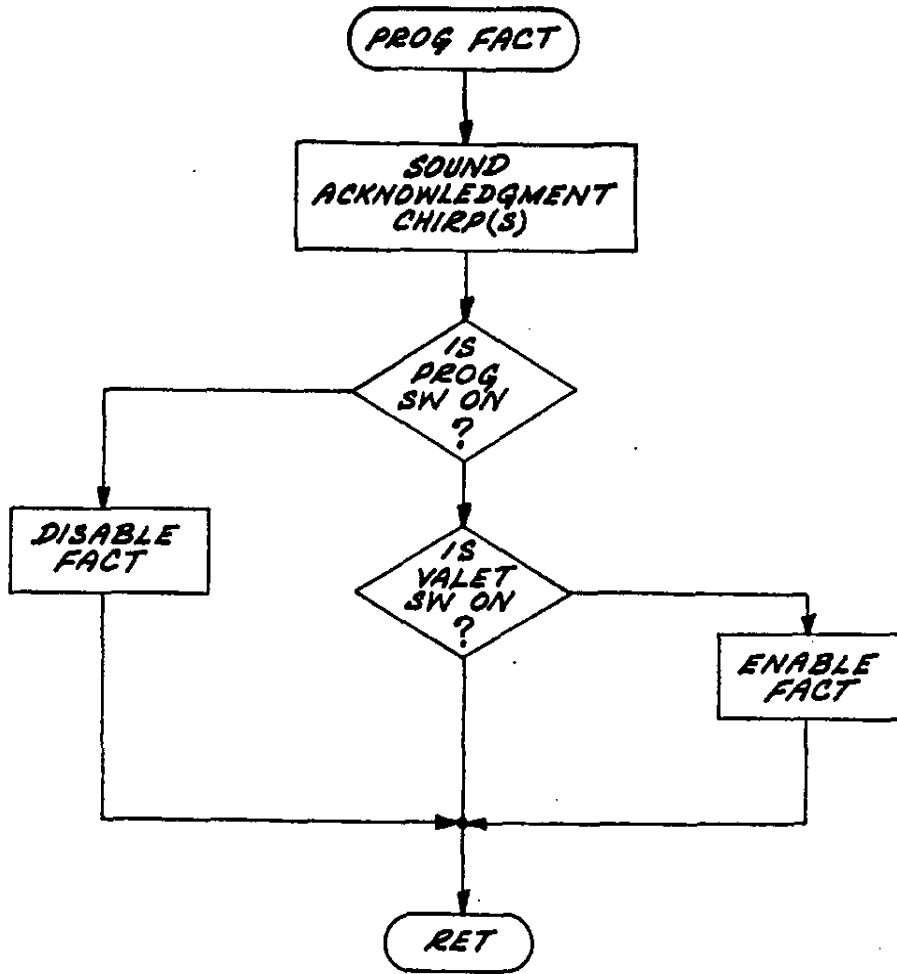


FIG. 15I

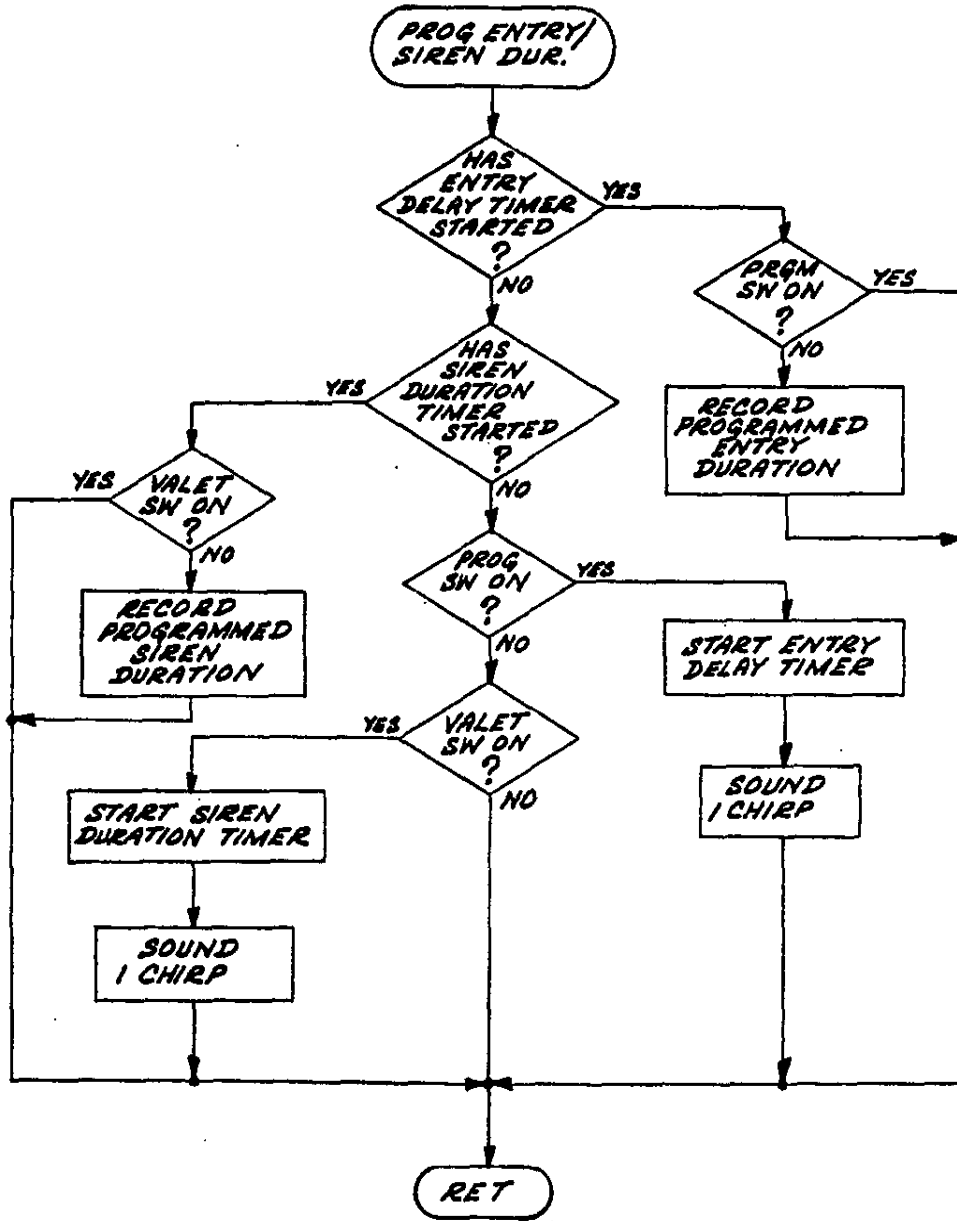


FIG. 15J

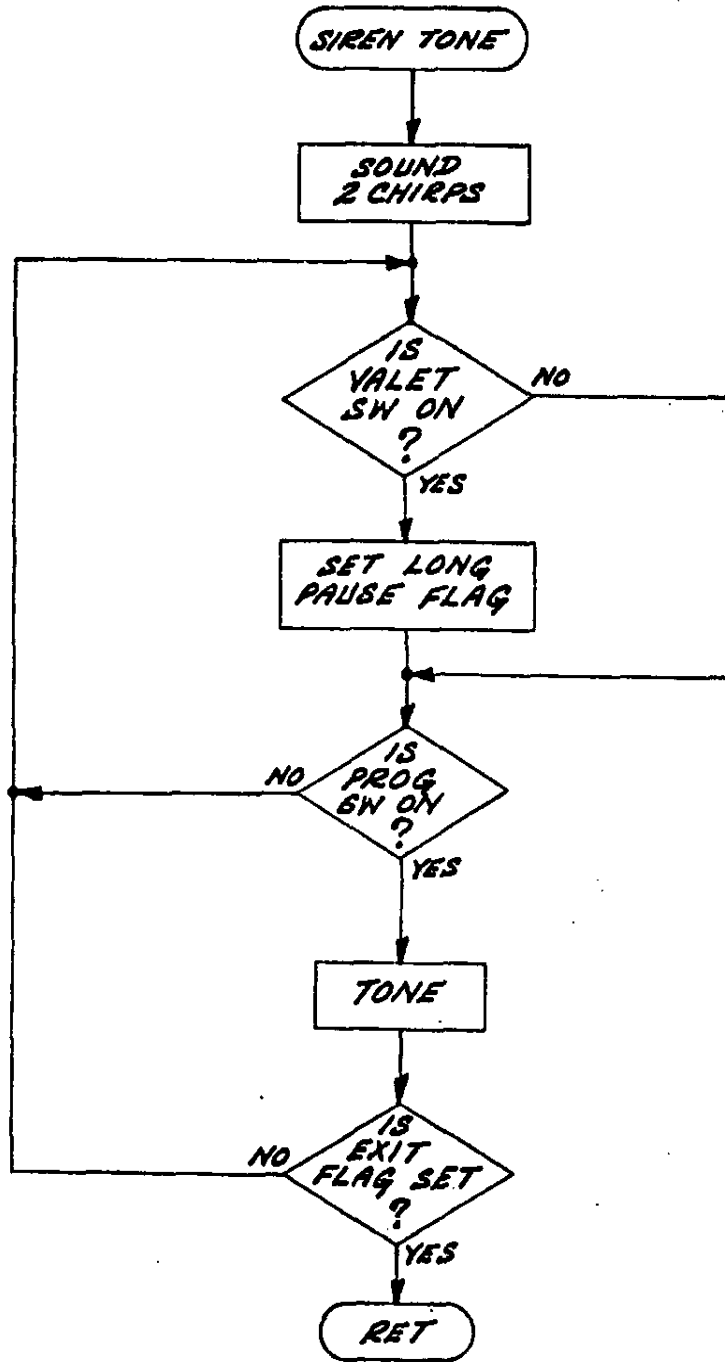


FIG. 15K

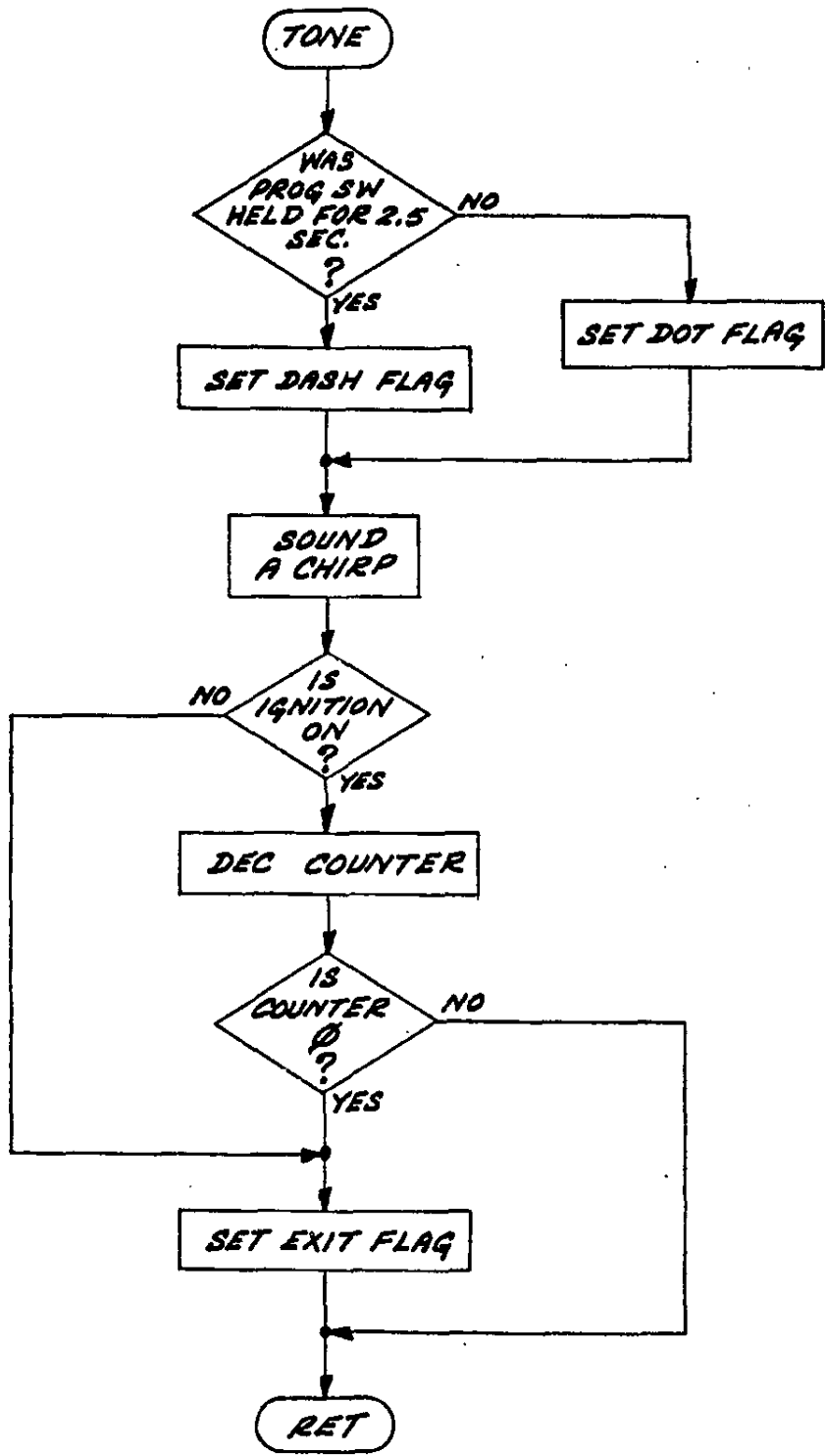


FIG. 15L

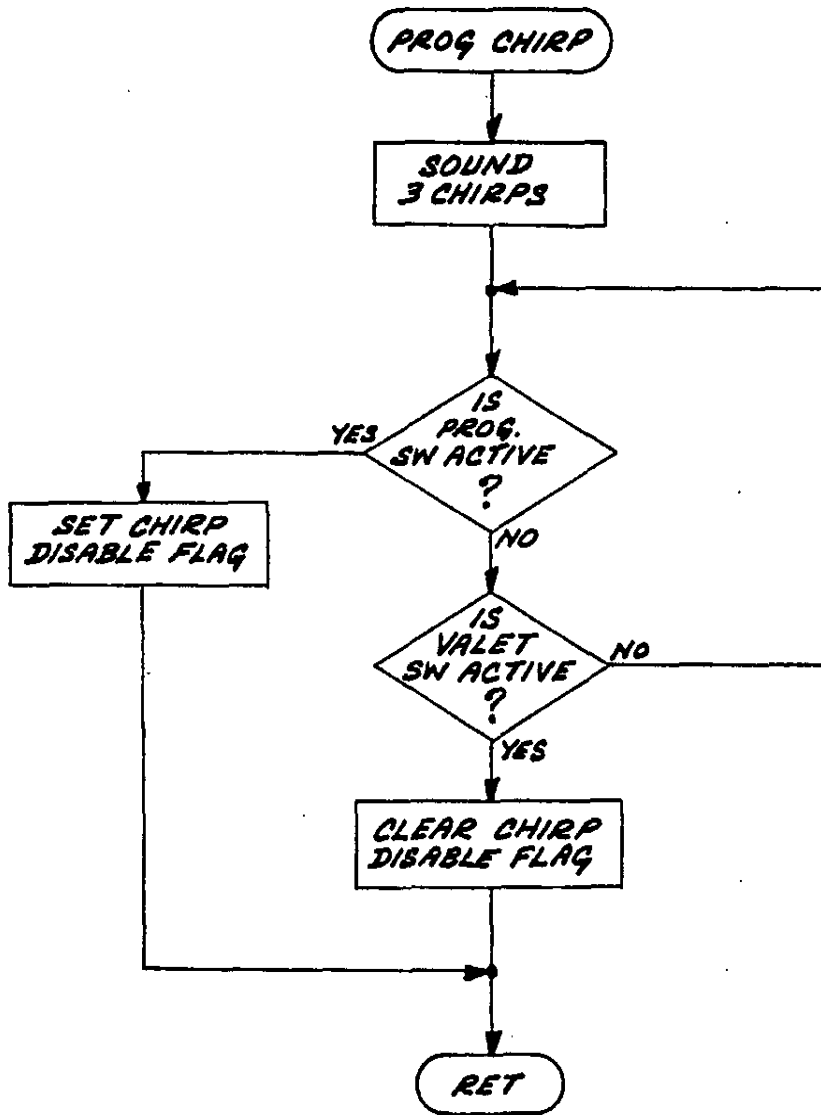


FIG. 15M

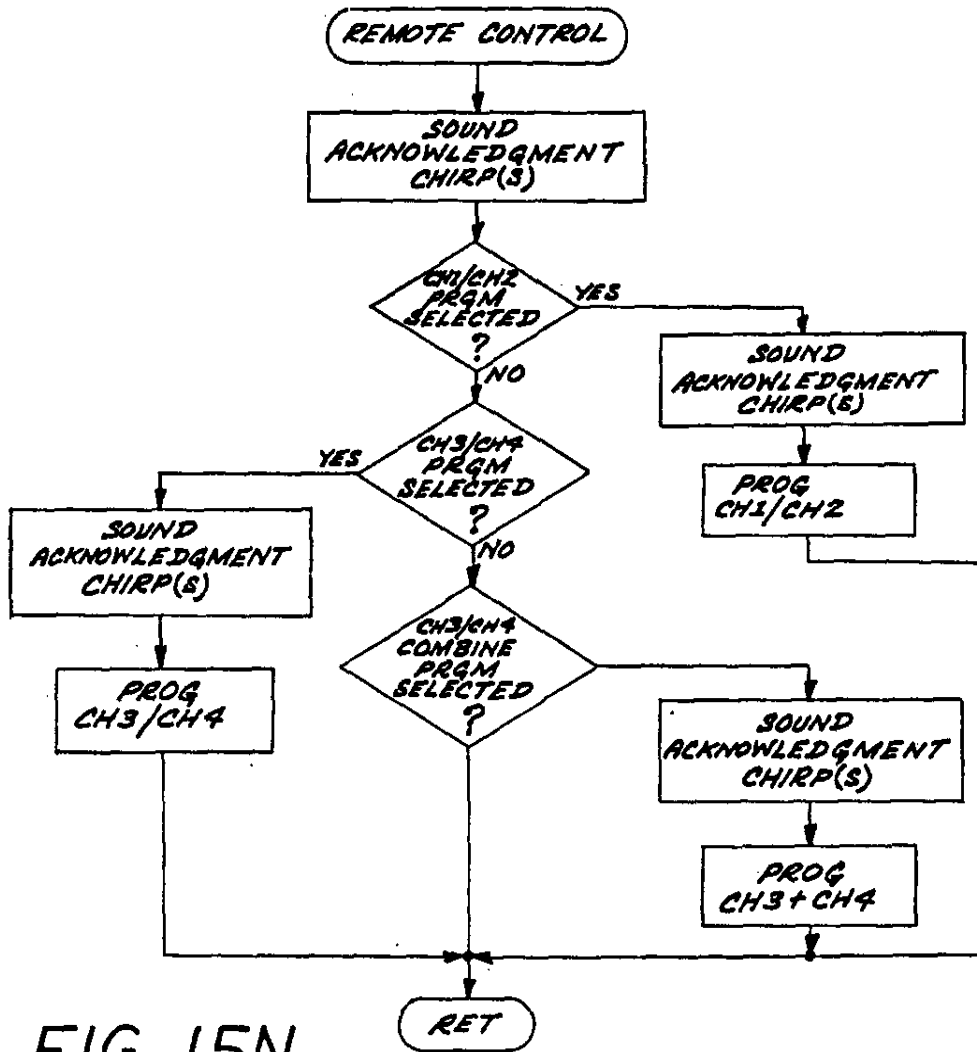
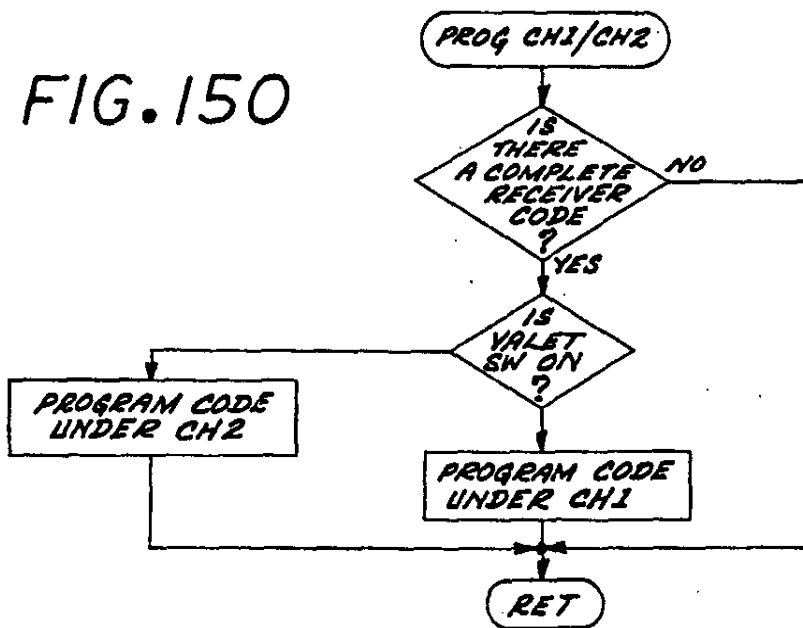


FIG. 15N

FIG. 150



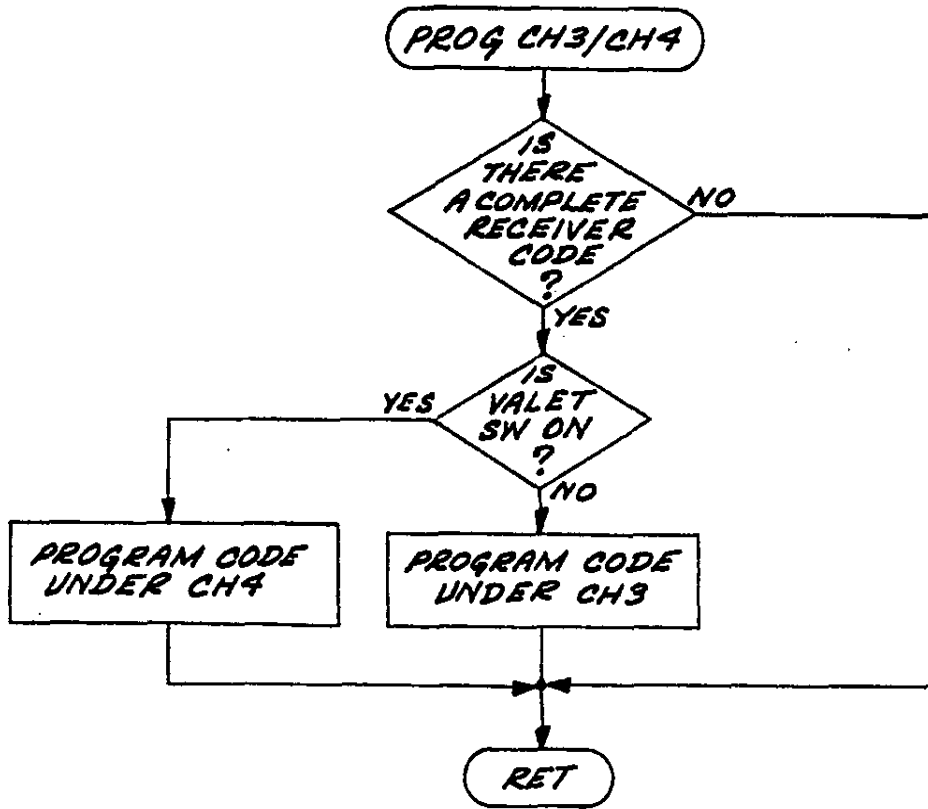


FIG. 15P

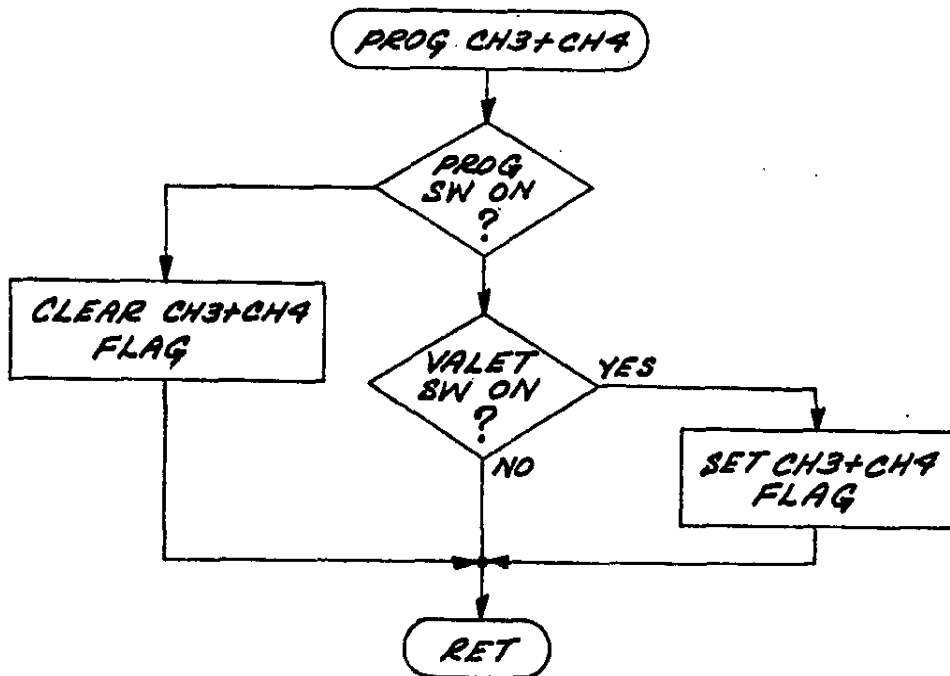


FIG. 15Q

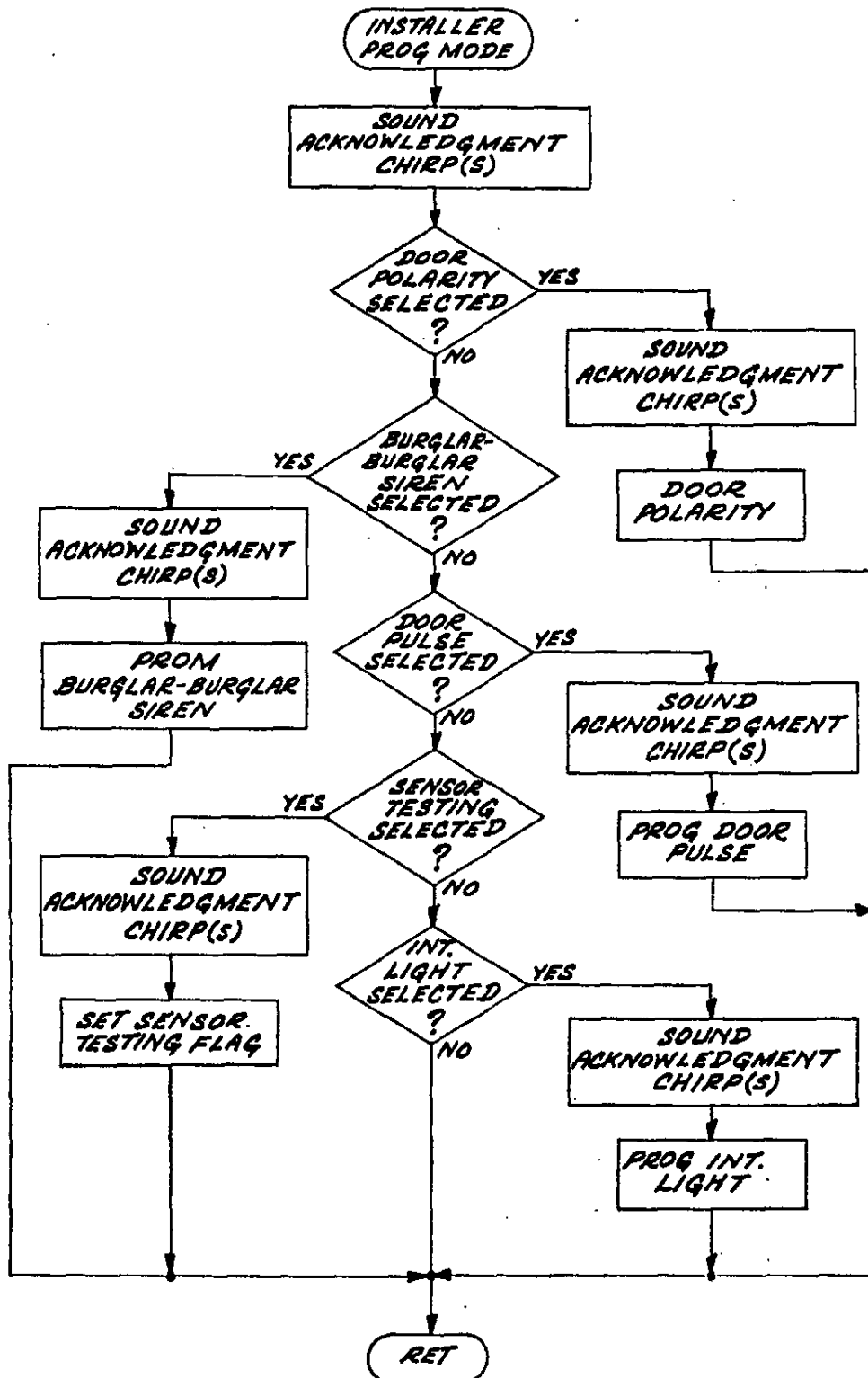
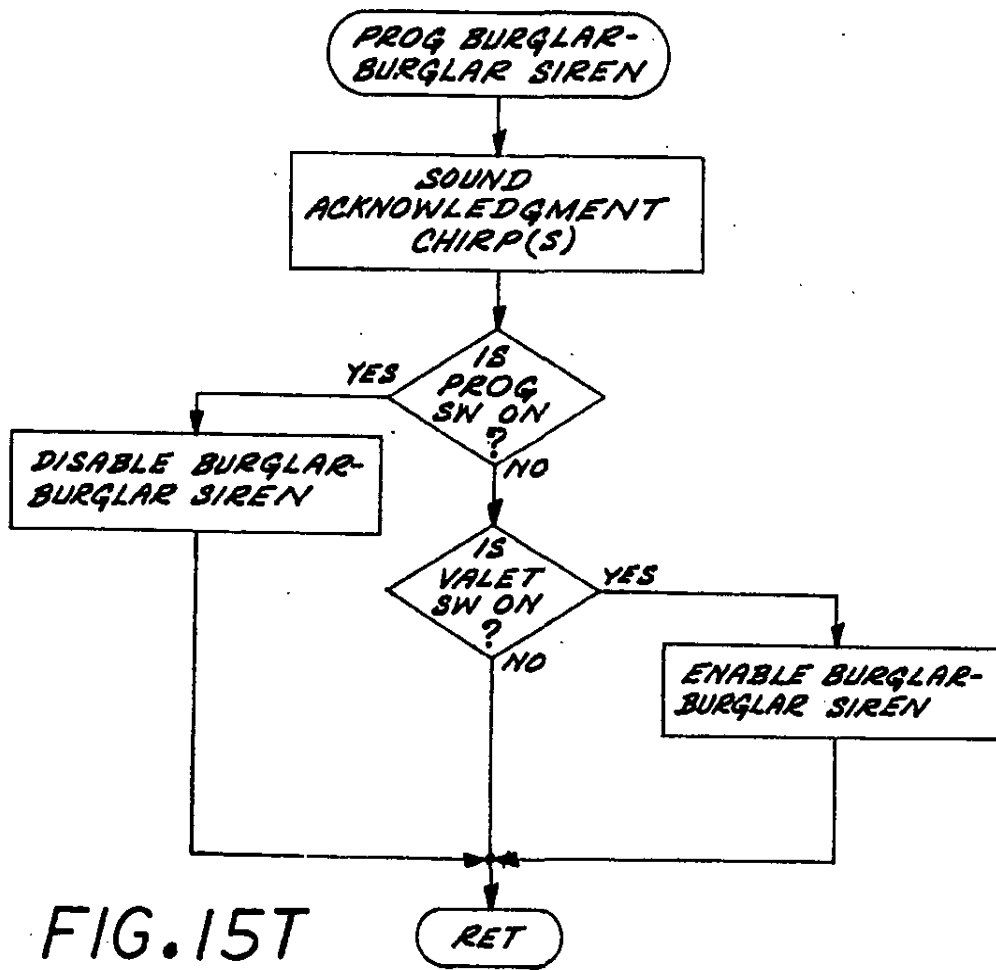
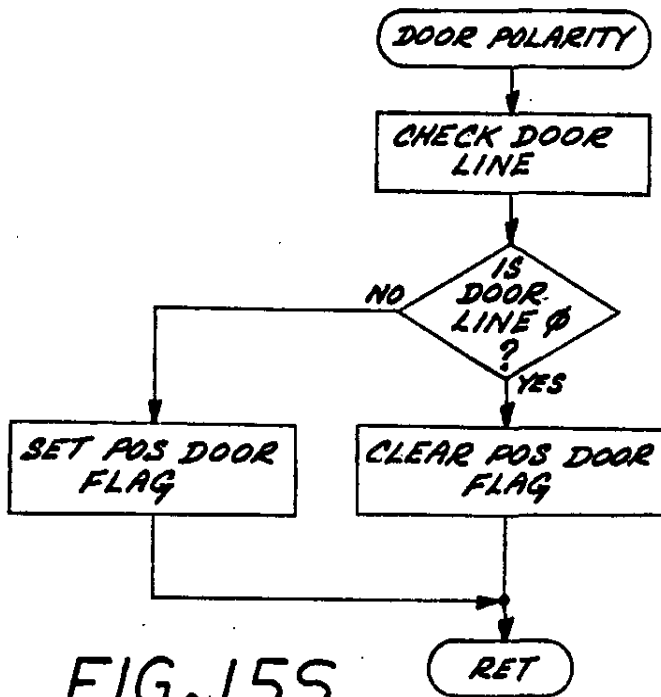


FIG. 15R



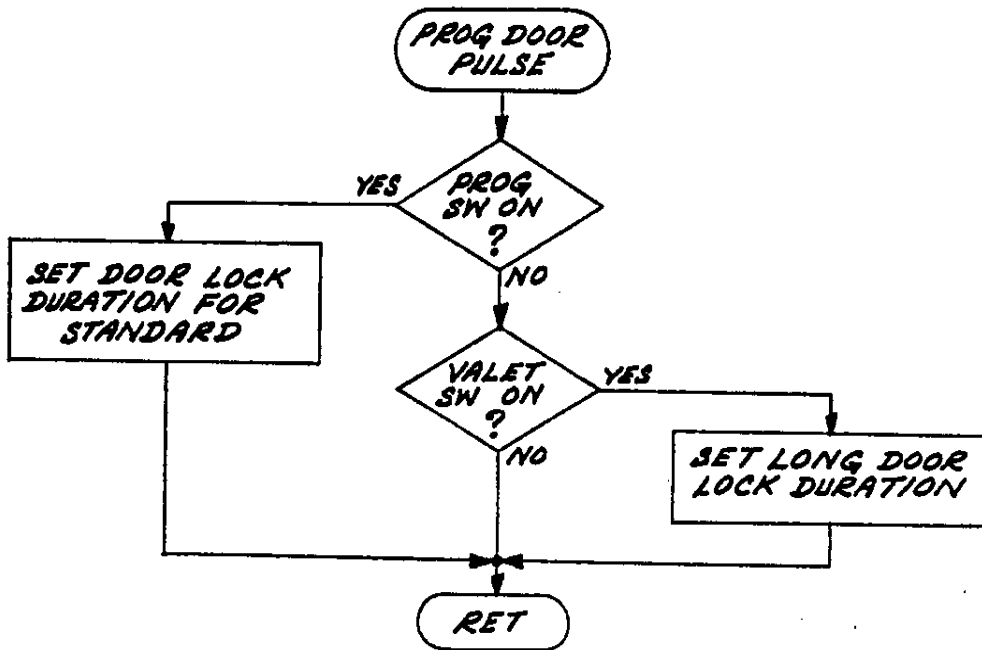


FIG. 15U

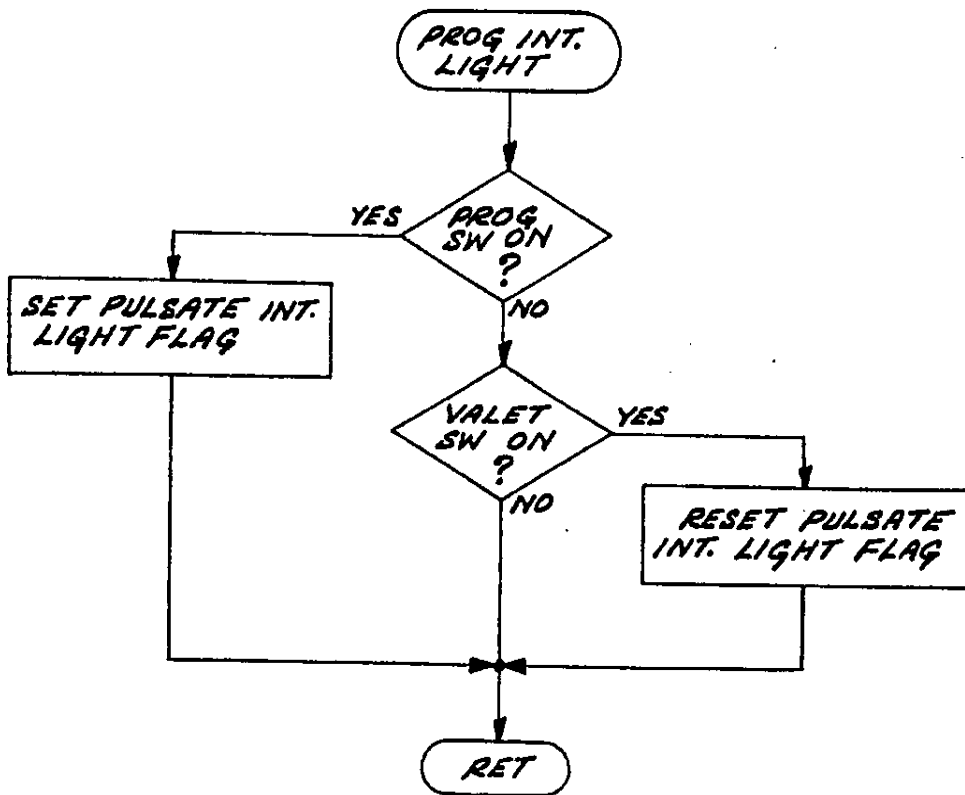


FIG. 15V

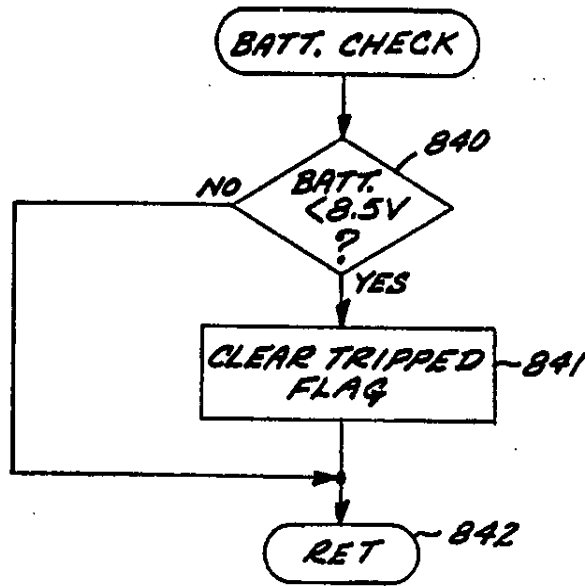


FIG. 16

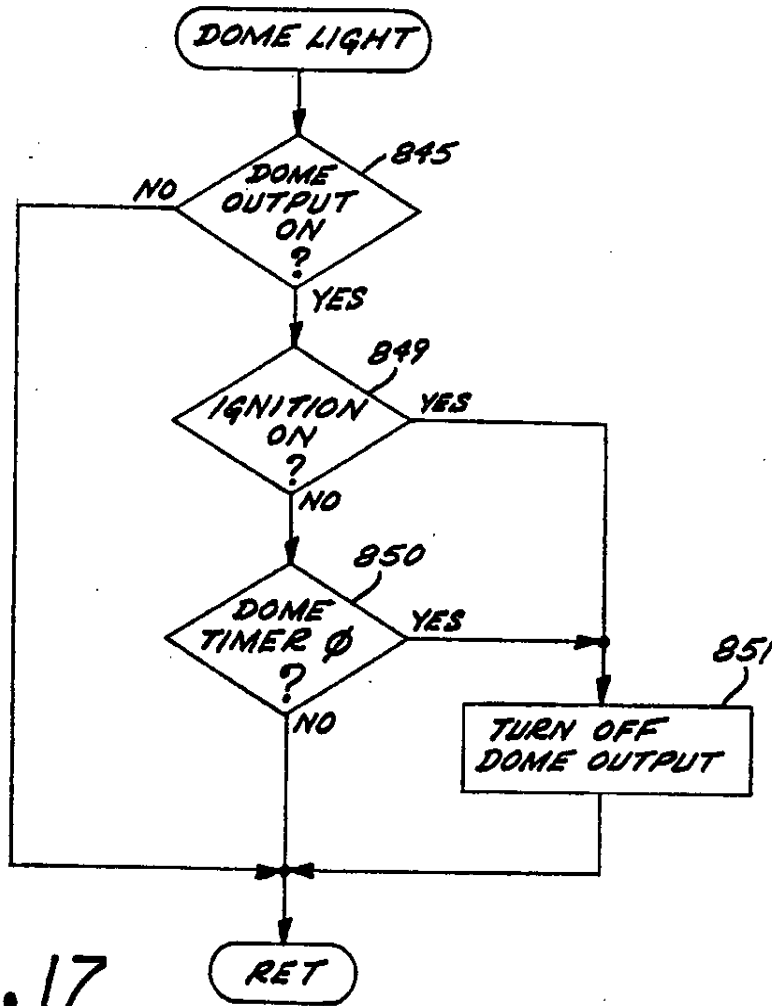


FIG. 17

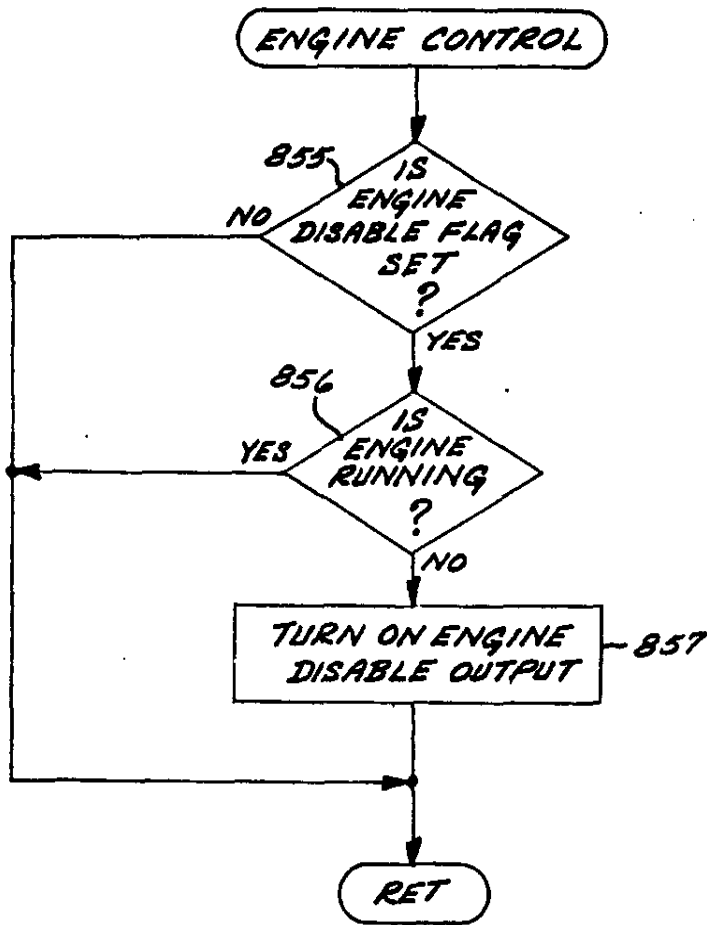


FIG.18

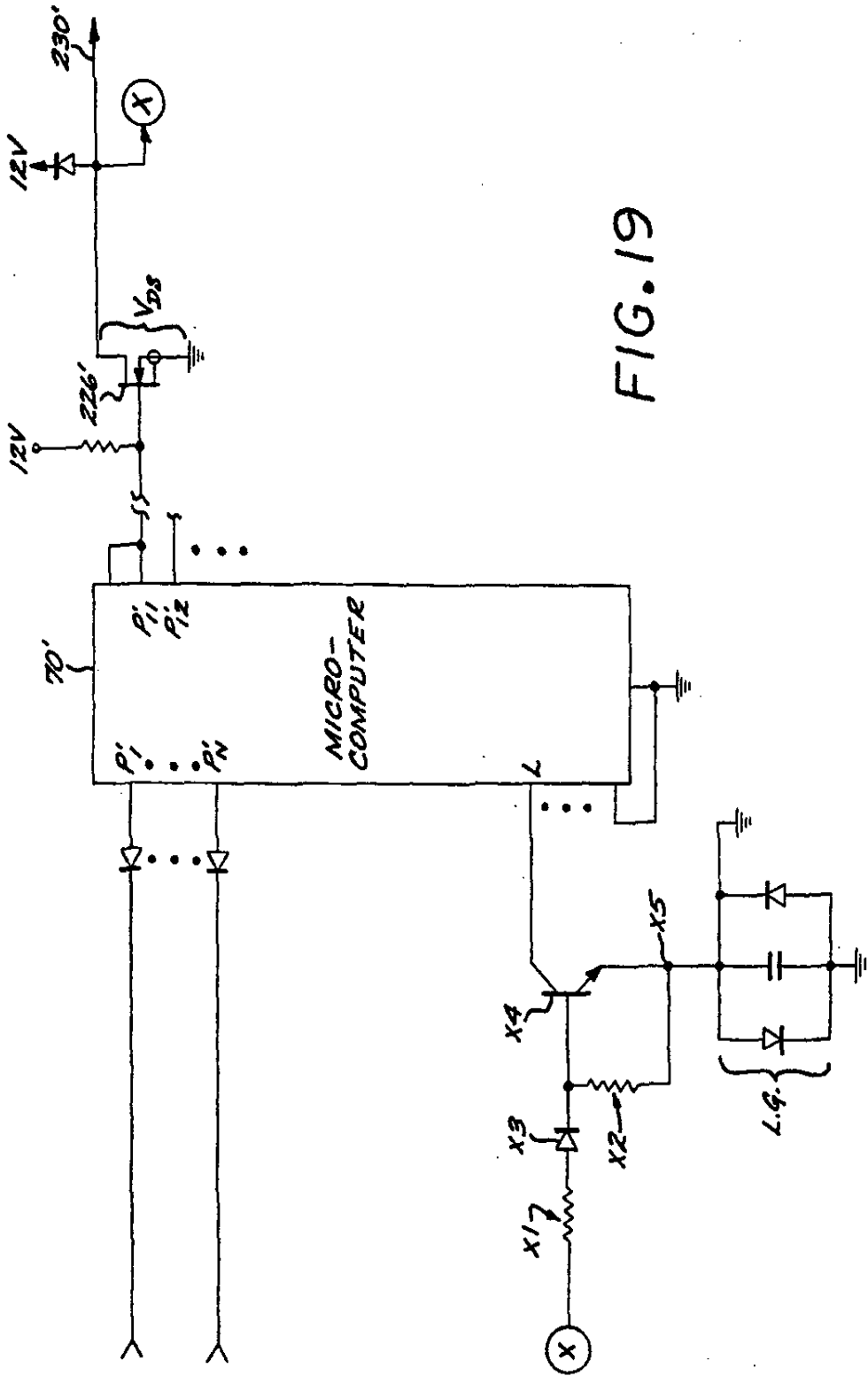


FIG. 19

ELECTRONIC VEHICLE SECURITY SYSTEM

This is a division of pending application Ser. No. 07/277,959, now allowed, entitled "Electronically Programmable Remote Control For Vehicle Security System" by Ze'ev Drori, filed Nov. 30, 1988, which is a continuation-in-part of Ser. No. 07/231,159, entitled "Electronic Vehicle Security System," by Ze'ev Drori and Amir Abrishami, filed Aug. 11, 1988, now U.S. Pat. No. 4,922,224, which is a continuation-in-part of application Ser. No. 07/138,828, entitled "Multi-Featured Security System With Self-Diagnostic Capability," by Ze'ev Drori and Mansoor Amirpoor, filed Dec. 28, 1987, now U.S. Pat. No. 4,887,064, all assigned to a common assignee with the present application.

BACKGROUND OF THE INVENTION

The present invention relates to the field of security systems for monitoring and controlling access to a secured or access restricted area, such as a vehicle.

Security systems are in wide use today to control and/or monitor access to secured or access-restricted areas. Such systems typically employ one or more sensors and/or trigger switches which are monitored or controlled by a central controller to sense intrusion or to allow controlled access. Examples of such systems include vehicle security systems and building security systems, which may be activated by either a remote switch or transmitter or by a key pad to enter a predetermined code. Entrance of the correct code typically arms or disarms the system, opens or closes a door or the like. Automotive security systems typically employ vibration sensors, glass breakage sensors, ultrasonic or microwave sensors, as well as triggers such as door, hood or trunk triggers, to detect unauthorized intrusion attempts and to activate alarm devices such as sirens or lights to warn off the intruder and call attention to the intrusion, and in most cases such system will also activate a relay or other electronic circuits disabling the vehicle ignition system.

The sensors and triggers typically detect attempts to intrude into the protected area, such as by way of a door or window, forcing a hood or trunk open, lifting or moving the vehicle or the like. The trigger devices may take the form of switches which are activated by the opening or closing of a door or window. To allow access through doors or other access points, devices which release or position locking elements, such as solenoid switches, are typically employed.

Conventional security systems will not arm when a sensor indicate that a door or window is open, or when a sensor indicates that there is presently an intrusion into the protected area. As an example, a vehicle door left open will typically prevent the security system from being armed, or a window left open in a building will prevent the building security system from being armed. For the same reason, a defective sensor which indicates that a door is open irrespective of the position of the door, i.e., open or closed, will also prevent the security system from being armed. The result is that the vehicle or building owner is deprived completely of the benefit of the security system until the defective sensor is repaired.

Another disadvantage of conventional security systems is repetitive alarm alerts due to conditions such as a defective sensor, or noncorrected or ignored intrusion events. Most systems on the market have a maximum

alarm duration for sounding a siren or other noise-making device when an alarm event is detected, after which duration the alarm resets itself. The maximum duration is typically set by local ordinances requiring that alarms shut off after some fixed time, say ten minutes, regardless of whether the owner has attended to the alarm or not. However, if the alarm was caused by a sensor or trigger which remains in an active state after the alarm system resets itself, then successive alarm cycles will be repeated over and over again until the alarm is disabled or the car's battery is depleted.

A further limitation of conventional vehicle security alarm systems is that they typically provide only a single type of audio alarm signal, such as a siren, or a siren sound alternating with a voice-synthesized audio message, e.g., "BURGLAR-BURGLAR." The same audio alert signal is generated no matter why the alarm condition was declared, e.g., a door opening results in the same alarm signal as a vibration sensor alarm condition. In many cases where the sensors cause an alarm, such as a vibration sensor or glass breakage sensor, a real intrusion event follows the sensor alarm condition within a few moments by the thief gaining entry through a door, trunk or hood. Yet because the same alarm audio signal results from both the sensor alarm and the door trigger alarm, the user may simply assume that the sensor alarm has caused the second alarm, not an actual intrusion into the vehicle, and ignore the warning.

Many luxury automobile are equipped with power door locks. Some electronic security and control systems have been integrated with the power door locks so as to automatically lock the doors when the security system is actively armed, and to automatically unlock the doors when the system is disarmed. However, a situation may arise where an inadvertent activation of the remote control will not only disarm the alarm, but also will unlock the vehicle doors.

It is therefore an object of the invention is to provide a system which does not repetitively cycle through alarm cycles due to a constantly active sensor or trigger device.

An additional object of the invention to provide a security system which provides a different type of alarm signal when a door is opened within a predetermined time interval after a sensor alarm condition is sounded.

A further object of the invention is to provide a security system with passive arming which automatically bypasses active sensor or trigger devices, thereby permitting passive arming to occur even in the presence of defective sensors or triggers and without triggering an immediate alarm.

Still another object of the invention is to provide a vehicle security system having remote control and passive control features with an intelligent automatic locking and relocking function, whereby the system will be passively armed and the doors automatically relocked if a door is not opened within a predetermined time interval after the system is disarmed.

SUMMARY OF THE INVENTION

These and other objects and advantages are provided by a security system as described herein. A security system is disclosed for monitoring and controlling access to a protected area, such as a vehicle. The system includes one or more sensor devices, each for sensing an intrusion event and providing a sensor activated signal when the event is detected. Such sensors may take the

3

5,157,375

form of vibration detectors, motion detectors, infrared, ultrasonic, or sound discriminators. The system further comprises one or more trigger devices, which may take the form of switches activated by the opening or closing of a door, hood, trunk or window.

The system further comprises means for communicating alert signals, such as for example, a siren, horn, auto-dialer for initiation of telephone calls or the like.

A system controller is provided to control the operation of the security system so that the system may be operated in an armed mode or in a disarmed mode. When in the armed mode the controller monitors the sensors and triggers and causes the communicating device to issue an alert signal through the output devices in response to a sensor or trigger activated signal.

In accordance with the invention, the system includes a means for reducing noise pollution and preventing the vehicle battery from being drained, due to repetitive alarms triggered by a constantly or repetitively activated sensor or trigger device. The system keeps track of the number of successive alarm cycles caused by activation of a sensor or trigger after the system was armed. Once this number reaches a predetermined maximum allowable number, the system will ignore any further activation signals from that sensor or trigger, and not generate alarm signals as a result, until the system is disarmed and rearmed again.

A further feature of the invention is to provide a first alert signal when a sensor device is activated after the system is armed, and thereafter to provide a more pronounced, second alert signal if any trigger is also activated within a given time interval after the sensor was activated. The first alert device may be a siren, and the second alert device may comprise a voice synthesizer for generating audible messages such as "BURGLAR BURGLAR." As a result, the system user is provided with clear alert indication signals that an intrusion has occurred.

Another feature of the invention is that triggers or sensors which are active when the security system is passively armed are automatically bypassed. This permits the system to be passively armed even if there is an active (typically defective) sensor or trigger and without immediately tripping the alarm due to such conditions.

The system further includes remote control door locking, unlocking and automatic relocking features that will automatically rearm the alarm and relock the doors if none of the doors are opened within a predetermined time after the system is remotely disarmed.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features and advantages of the present invention will become more apparent from the following detailed description of exemplary embodiments thereof, as illustrated in the accompanying drawings, in which:

FIG. 1 is a simplified block diagram of a security system employing the present invention.

FIG. 2 is a schematic diagram of the receiver circuit of the security system depicted in FIG. 1.

FIG. 3 is a schematic block diagram of the controller and input and output buffers of the security system of FIG. 1.

FIG. 4 is a schematic diagram of a reset signal generating circuit employed with the controller of FIG. 3.

FIGS. 5A and 5B are schematic diagrams of LED driver circuits employed with the controller of FIG. 3.

4

FIG. 6 is a circuit schematic illustrating an embodiment of the power supplies employed in the system of FIG. 1.

FIGS. 7-18 are flow diagrams illustrating the operation of the security system generally depicted in FIG. 1.

FIG. 19 is a simplified circuit schematic illustrating the output protection circuitry comprising the output protection feature of the invention.

DETAILED DESCRIPTION OF THE DISCLOSURE

A simplified block diagram of the principal structural elements of a system embodying the invention is set forth in FIG. 1. The system includes a means for permitting the user to communicate with the system controller 70. This communicating means may take the form, in the conventional manner, of a transmitter device 55 for transmitting an encoded signal via an antenna 56. The transmitted signal is received by receiver 65 via antenna 66, and the received signal is provided in some form to the system controller 70. Additionally, or alternatively, the user communicating means may take the form of a key pad 60, which is coupled directly to the controller 70 by cable 62. The keypad 60 may comprise a plurality of digit keys 1-9, as well as additional keys or switches employed for various functions such as an "armed" switch for signaling the system to enter the armed mode. Additionally, or alternatively, the user communicating means may take the form of one or more switches 77 manually manipulated by the user. Such switches may take the form of a single three-position toggle switch having an off position intermediate a "momentary" position or switch spring-loaded toward the off position and a "valet" position or switch. With the transmitter 55, which may be used remotely, the keypad 60, or the program switches 77, the user may input to the controller a predetermined coded message to cause the controller to initiate some action, e.g., arming or disarming the security system, sounding an alert, entering the programming mode, or the like. One type of coded message typically takes the form of a predetermined sequence of binary-valued signals, which collectively define a digital user authorization code, e.g., a predetermined N-bit word. One aspect of the invention, the branch programming feature described below, is advantageously employed with a system employing a transmitter and the three-position switch but without a keypad.

Power supplies 95 provide electrical power to the receiver 65 and the controller 70. In the case of a security system mounted in a vehicle, the power supplies receive the primary source of power from the vehicle battery, typically 12 volts, and convert that available power source into voltage levels required by the system, here regulated +5 volts and +8 volts.

The system triggers and sensors 75 are coupled to the system controller 70 through input buffer circuitry 80. In the case of a security system installed in a vehicle, the sensor elements may be motion or vibration sensors, glass breakage sensors, ultrasound sensors and the like. The triggers are hard-wired switches on the doors, hood and trunk lid activated by a particular event such as opening or closing a door.

The system 50 further employs a plurality of controlled devices, indicated generally in FIG. 1 as elements 90, which are coupled to the system controller by output buffer circuitry 85. In the case of a vehicle security system, the controlled devices may include one or

more of the controlled devices 90 shown in FIG. 1, i.e., the voice synthesizer 91, siren 92, pulsed alarm 93, (hooked to parking light and/or air horns), door lock device 94, door unlock device 95, hood lock device 96, accessory 97, starter or ignition cutoff apparatus 98, LEDs 99, telephone autodialer 100, and the vehicle interior courtesy or dome light 101.

The transmitter 55 in a preferred form provides a pulse-width-modulated RF signal, wherein an RF carrier at some predetermined RF frequency is modulated by information from an internal encoder unit. As is well known in the art, the transmitter may be actuated by depressing a switch, thereby generating a transmit signal encoded with information such as a multi-bit code. The specific code may be determined by the status of switches or the like comprising the encoder. The width of each pulse determines its status as a digital "1" or "0." The particular circuit arrangement comprising the transmitter 55 per se forms no part of the invention, and is not described herein in further detail. An exemplary circuit arrangement is described in the co-pending application entitled "Electronically Programmable Remote Control Access Systems" by Ze'ev Drori, Ser. No. 094,395 now abandoned, the contents of which are incorporated herein by this reference.

The receiver 65 is more fully illustrated in FIG. 2, and is described in U.S. Pat. No. 4,887,065, the contents of which are incorporated herein by reference.

The output of the receiver 65 from inverter 160 is introduced into the controller 70, as is more fully illustrated in FIG. 3. In this case, the output from the receiver 65 is introduced into an exclusive OR gate 162 (acting as a programmable inverter) which has an output to the controller 70. The controller 70 comprises a microcomputer, with some internal RAM and nonvolatile memory capacity, such as the NEC 80C49H microcomputer.

The plurality of sensors and triggers 75 (FIG. 1) are coupled to the controller 70 by a buffer circuit 80 comprising the diode network 212 shown in FIG. 3. The triggers and sensors 75 are connected to nodes 201-210 which connect to the network 212 and to node 211. By way of example only, a door trigger device may be connected to node 201, first and second sensor devices to nodes 202 and 203, an "immediate" trigger device at node 205, a hood position sensor at node 206, program switches 77 (the "valet" and "hood" switches) at nodes 208 and 209, a normally closed trigger at node 210, and an ignition switch "on" or "off" sensor at node 211. Commonly, the door trigger node is actually wired to the vehicle interior light, which is in turn activated by the conventional door trigger switches. The pins P1-P8 are monitored by the microcomputer 70, enabling the microcomputer to monitor the states of the trigger and sensor devices, thereby monitoring the protected areas of the vehicle.

The particular triggers, sensors and switches are described by way of example for a vehicle security system implementation. The "immediate" trigger device is typically connected to the vehicle trunk or back door, for generating an immediate alarm when the trigger is activated. The hood position sensor provides a signal indicative of the position of the hood, i.e., closed or not closed. The normally closed trigger coupled to node 210 is a trigger device that is normally grounded, and is activated when the trigger is no longer grounded. Such a trigger is normally connected to the vehicle radio, to signal when the radio has been removed.

The sensors and triggers 75 and switches 77 are preferably coupled to the controller 70 in such a way as to allow the controller to monitor the individual status of each device. Pin P10 of the microcomputer 70 is also monitored to receive information from the receiver 65.

Pins P11-P20 of the microcomputer 70 are employed as output pins to control the various controlled devices 90 employed with the system. The output buffer circuitry 85 comprises hex driver device 214, for example, a type 76C906 device, and pullup resistor network 216 connected to output lines 218-223, which are in turn connected to a corresponding plurality of power T MOS transistor output devices, one of which is indicated as device 226. The output of the power transistor 226 is diode-coupled to a 12 v power source and is connected to a controlled device at node 230. Thus, the driver circuit 214, network 216, power transistor 226 and diode connection to the power source serves as part of the output buffer circuit 85 to enable the low level microcomputer output signals to drive a controlled device such as, for example, a siren, pulsed alarm, door lock, door unlock, a hood lock, and the like which require substantial power to operate, e.g., by actuating relays. Nodes 231-235 are connected to similar power transistor output devices, which for the sake of clarity are not shown. These nodes are also used to control various controlled devices.

For this example of the invention, line 218 controls the siren device 92, line 219 the pulsed alarm 93, line 220 the door lock device 94, line 221 the door unlock device 95, line 222 the hood lock device 96 and line 223 an accessory device 97, the interior light 101, or the autodialer 91.

Another output pin P20 of microcomputer 70 is coupled to an inverter circuit 238 whose output is connected to driver transistor 240. The collector of transistor 240 drives power transistors 242 and 244 to provide additional control nodes 248-250 to control various controlled devices, such as the starter/ignition cutoff device 98, accessory 97 and the like.

Output pins P17-P19 are connected respectively to the circuit shown in FIG. 4 and the LED driver circuits of FIGS. 5A and 5B.

An oscillator circuit 252 provides a stable oscillator frequency signal to the microcomputer for use as the device clock. The microcomputer 70 receives +5 volt power from battery circuit 254 and from power supplies 95.

The microcomputer 70 receives a reset signal on pin P21 from a reset signal generating circuit shown in FIG. 4, and described more fully in U.S. Pat. No. 4,887,064.

FIGS. 5A and 5B illustrate respective driver circuits for the green and red LED devices 99 which are employed in the disclosed embodiment to provide a means for visually communicating with the user of the system. Pin P18 of the microcomputer 70 controls the green LED driver circuit of FIG. 5A and pin P19 controls the red LED driver of FIG. 5B. The green LED driver circuit comprises an inverter device 272, NPN transistor 274, PNP transistors 276 and 278 connected in the manner shown in FIG. 5A. The operation of the driver circuit of FIG. 5A as well as that of FIG. 5B will be readily understood by those skilled in the art. In the case of the security system installed in a vehicle, the LEDs 99 may be mounted on the vehicle instrument panel or dashboard.

Referring now to FIG. 6, the circuitry for the power supplies 95 is shown. The circuitry develops regulated 5

5,157,375

7

and 8 volt sources. By monitoring the state of the regulator error signal at pin P23, the controller determines when the +8 volt supply is no longer available. In such case, the controller will disable operation, as is described more fully in U.S. Pat. No. 4,887,064.

To further explain the operation of the system shown in FIG. 1, a general flow diagram is set forth in FIG. 7. As will be apparent to those skilled in the art, the desired operation of the system is achieved by appropriate programming of the controller 70 to achieve the functions indicated in the flow diagram.

The operation commences at step 400 on system powerup with the RESET function. This results in the reset circuit (FIG. 4) providing a reset signal to the controller to initialize the various parameters and flags utilized in the microcomputer 70. The reset function also includes detecting whether power has been disconnected from the security system and then reconnected. The system will activate the alarm if the reconnection of power is unauthorized. The "reset" feature of the system is more fully described with respect to FIG. 8.

The next step 404 in the general operational flow is to decode the received RF signal, in the case of the embodiment of FIGS. 2-6, wherein decoding internal to the microcomputer 70 is employed. This function is a correlation of the received sequence of digital data bits with the stored authorization code. If the received signal matches the stored code, then a flag is set indicative of the condition of a correctly entered user authorization code. The decode function for the internal decoder is interrupt driven, with assembly of the incoming data bits occurring in the background until a "dead period" is detected with no data coming in for a predetermined period of time. Then the received bit sequence is compared with the stored data, and flags are set accordingly. The internal decoding function is shown more fully in FIGS. 9A-C.

The next function to be performed is the ALARM mode function 406. Here, the alarm mode is commenced, if appropriate, as determined by the appropriate software flags, i.e. the "TRIP" or "PANIC" flags. Thus, if the alarm mode has been triggered, then controlled devices such as the siren, the dome and parking lights and the like as programmed to occur during an alarm event are activated. The alarm mode starts a timer for the alarm duration. If either the "PANIC" or "TRIP" flag is cleared during the timeout, the alarm mode ends immediately. Otherwise the flags are cleared at the end of the alarm interval. The alarm mode is described more fully with respect to FIG. 10.

The next function in the overall sequence is the VALET MODE function 408. The valet mode allows the security system to be disabled so that the vehicles may be left in the care of an authorized person, such as a valet, service technician or the like. Thus, if the valet mode is properly entered, the VALET flag will be activated.

The next function 410 to be accomplished by the system is to check the triggers and sensors of the system. This is accomplished by reading the states of the microcomputer 70 pins P1-P9. For each active line or device, a flag is set. The flag will be cleared when the particular line or device is no longer active.

The next function in the main loop (FIG. 7) is the CONTROL function 412. This is described in detail with respect to FIGS. 11A-11C. In general, the control function responds to the decoder outputs. When the command is received to arm the system, the controller

8

checks the sensor and trigger flags. If no sensor or trigger line is active, i.e., none of the device flags are set, then the controller enables two "chirps" (a chirp is sounded by a pulse applied to the siren 92) and then sets the ARMED flag. If there is an active trigger or sensor, four chirps are sounded and the controller provides information to an LED register comprising the controller 70, indicating which sensor is active, i.e., setting a flag which will be used to communicate visually to the user which sensor is defective. If the decoder signal is to disarm the system, then the controller sounds one chirp if there was no tampering with the controlled area. If tampering occurred during the time the system was armed, the chirp counter is set to 3 (step 563, FIG. 11B), the controller 70 provides the LED register with information as to which sensor or trigger was tampered with (step 564). During this function the controller also sets the duration for the door unlock/lock signal.

Once the CONTROL function has been completed, then at step 414, the decision is made as to whether the system is armed, by checking the ARMED flag. If the system is armed, then the next function is the armed mode function 418. If the system is not armed, the disarmed mode function 416 is performed.

A timer is initiated in the ARM mode (FIG. 11D) to disable the sensor "two" (e.g., a motion or shock detector or sound discriminator) line (coupled to pin P2 of the controller 70 in FIG. 3) for five seconds. After the initial five seconds, both trigger and sensor lines are enabled. A counter function is provided for counting how many times each sensor or trigger is activated consecutively. After ten consecutive alarms by a particular sensor or trigger, that device will be disabled. This prevents noise pollution and battery drain caused by what would otherwise be a continuing alarm signal. If a sensor or trigger is active, a TRIP flag is set and information is placed in a register which identifies the particular trigger or sensor which tripped the alarm. The LED control mode 420 responds to this data when the system is disarmed.

The DISARMED function 416 controls the passive arming of the system. This is described in further detail with respect to FIG. 15B.

The LED control function 420, when the system is armed, sets the red LED flag to flash with the appropriate message as indicated by the data stored in the LED register. If the system is disarmed, the green LED flag will be set to flash in the appropriate sequence. If the valet mode has been entered the green LED flag will be set. The LED control is shown in further detail in FIGS. 14A-C.

The next function in the general operation flow is the OUTPUT CONTROL function 422. Here the controller examines the flag for each output line of the controller 70 for a controlled device, and if set, will turn that output line on. If the flag for a particular output line is cleared, the controller will turn that line off. Thus, this function activates and deactivates the controlled devices 90, in dependence on the state of the software flag associated with the particular device.

Following the OUTPUT CONTROL function 422, the OUTPUT PROTECTION function 423 is performed. This function involves monitoring the current flow magnitude through particular controlled devices, generally the siren and the ignition cutoff devices, and turning off these devices if the current through a respective output device exceeds a predetermined level. This protects the output devices against damage due to im-

proper installation or wiring conditions. This feature of the invention is described more fully with respect to FIG. 19.

The next function is the CHECK SWITCHES function 424. During this step, the controller checks the status of all switches other than sensors and triggers, i.e., the ignition switch, and the ("valet" and "program") switches 77. The controller sets flags as appropriate for each line.

The next function is the ENTER PROGRAM function 426. The purpose of this mode is to program the system, e.g., by enabling or disabling particular programmable features of the system as is described more fully with respect to FIGS. 15A—U. The system chirps once to signify that the program mode has been entered and the green LED is turned on. The programming mode can be aborted by turning the ignition switch off.

The CHECK BATTERY function (step 430), shown in FIG. 16 operates to detect the condition wherein +5 volts is not available to the security system, and disables the system in that event to avoid further draining the vehicle battery. The DOME LIGHT function 432 allows the user to have the interior courtesy or dome light activated for a predetermined interval after the system is disarmed or until the ignition switch is turned on. Another function performed during the main loop is the "ENGINE CONTROL" function 434. This function selectively disables the vehicle engine to prevent unauthorized operation of the vehicle.

After step 434 has been performed, the operation flow loops back to step 402 to commence the loop again. The entire main loop takes only a short period of time to complete, on the order of milliseconds.

Selected ones of the particular functional modules described above will now be described in further detail. FIG. 8 shows the RESET module which is activated when the +5 volt power supply to the system 50 is interrupted and restored. Upon power up, the controller 70 input/output lines are initiated at step 450. At step 452, the registers of the random access memory of the controller are initialized. At step 454, the ignition switch state is read and if turned on, the ARM flag is cleared at step 456, and the program operation returns to step 402 of the main operation loop. If the ignition switch is not turned on, the ARM and TRIP flags are set, since this is interpreted as an unauthorized power up of the system, and program operation returns to step 402.

The internal DECODE module 404 is illustrated in further detail with respect to FIGS. 9A—B. FIG. 9A shows the bit assembly operation carried out by the controller 70 as data is being received by the receiver. This background operation is continuously performed, even as the operational flow is at various functions within the main loop of FIG. 7. The receipt of a bit (rising edge) from the receiver at pin P10 of controller 70 results in a hardware interrupt, which shifts operation to the bit assembler (FIG. 9A). At step 462, if a rising edge of a received pulse is detected, then at step 464 a "bit width" timer is started, the bit count for the particular received sequence of bits is incremented (step 466), and at step 470 operation returns to whatever step in the main loop in which the interrupt occurred. If at step 462, the rising edge of a pulse is not detected, then at step 472 the present pulse width is determined, and if not within the predetermined limits (step 474), then at step 476 an ERROR flag is set. At step 470 operation returns to the main loop step at which the interrupt

occurred. If the pulse width is within limits, then at steps 478, 480 and 482 either a "1" or a "0" bit is assembled with the preceding data bits, as appropriate. At step 484, the "dead period" timer (10 milliseconds) is reset and at step 470 program operation returns to the main loop.

Referring now to the DECODE subroutine of FIG. 9B, the first step 490 is to determine whether a complete word has been received. This determination is made upon occurrence of a "dead" period by checking the bit count and comparing that current count with the length of the authorization code. If a complete word has not been received, then the subroutine returns to the main loop. If a complete word has been received, then at step 492, the received word is compared against the stored authorization codes to determine if there is a match. If not, the program operation returns to the main loop. If the received word matches any of the programmed authorization codes, then if the matching code has been received twice consecutively (step 494), the decoder is activated at step 496. If the matching code has not been received twice consecutively, program operation returns to the main loop without activating the decoder. The requirement that the matching code be received twice consecutively is a further security feature, against the user of code scanners.

A "dead period" timer is employed as a "background" function, which on an interrupt basis monitors the receiver output to locate 10 millisecond time periods between received data. Such gaps indicate that a data word has been received. The dead period finder function is illustrated in FIG. 9C. The routine employs a 10 millisecond software timer, which is reset during the bit assembler operation (step 484, FIG. 9A). At step 501, this dead period timer is checked to determine if it has received the "0" timed-out state. If not, the operation returns to the particular function in the main loop at which the interrupt occurred. If the timer state has reached "0", then at step 502, the bit count is checked to see if the bit count is not equal to the maximum possible code bit length. If the count equals that maximum length, then the decoder is reset to the inactive state at step 506, and the operation returns to the main loop. If the bit count does not exceed this maximum length, then the error flag is checked at step 503, and if set, operation branches to step 506 to reset the decoder. If the error flag is not set, then at step 504, the assembled word is stored (step 504) in a buffer memory comprising the controller 70, the completed word timer is reset at step 505, the decoder is reset to the inactive state (step 506), and operation returns to the main loop.

The ALARM mode function (function 406 in FIG. 7) is shown in FIGS. 10A—D. This function is to activate and deactivate the alarm condition events at the appropriate times. At step 507, the alarm flag is checked. If set the alarm timer state is checked (step 508A) to determine whether it has reached the "0" or timed-out state. If the timer state is "0," then the ALARM, TRIPPED and PANIC flags are cleared (step 508B), the controller outputs for the controlled alarm devices are turned off (step 508C), and operation returns to the main loop. If the alarm flag is not set (step 507), the TRIPPED and PANIC flags are checked at step 509. If neither flag is set, no alarm devices are to be activated, and therefore operation returns to the main loop. If either the TRIPPED or the PANIC flag is set, then at step 510, the ALARM flag is set. At step 511, the alarm timer is loaded with the programmed alarm duration, and then

5,157,375

11

the alarm outputs are turned on (step 512A), including such controlled devices as, for example, the siren, pulsed alarm, autodialer and vehicle interior light. At step 512B, the "BURGLAR-BURGLAR" subroutine is called. Its purpose is to activate a second alarm device if certain conditions are met, the second alarm device (e.g., device 91, FIG. 1) comprising a siren and voice-synthesizer device, now commercially available, which alternates a siren sound with the voice synthesized audio message "BURGLAR-BURGLAR." The subroutine 512B is described more fully with respect to FIG. 10E. If at step 512C, the BURGLAR-BURGLAR siren is active, the siren subroutine 513 is bypassed. Steps 513 and 514 indicate the SIREN and PULSED ALARM subroutines, the former illustrated in FIGS. 10C-D. Lastly, the INT LIGHT subroutine is called at step 514A, and illustrated in FIG. 10F. If this feature has been enabled by the installer, the interior light will be pulsed on and off during an alarm cycle. Operation then returns to the main loop.

The first step of the SIREN subroutine (FIG. 10B) is to determine whether the siren counter is at the "0" state (step 515). If not, the counter is decremented (step 516) and its state is again checked. If the count is "0," at step 525, the timer variable TSIREN is set to 240 milliseconds, the siren output line is turned off (step 526). Operation then returns to the main loop. If at step 515, the counter is at "0," then the siren counter is reset (step 521), TSIREN is set to 2.5 seconds (step 522) and the siren is turned on (step 523) before operation returns to the main loop. At step 517, if the counter state is not zero, then through step 518, either the OFFSOUND or ONSOUND subroutines (FIG. 10C and 10D, respectively) will be accessed. At step 520, operation for the next bit in the personalized siren code is set up, and operation returns to the main loop.

The first step 530 of the OFFSOUND routine (FIG. 10C) is to turn off the siren. The bit status of the programmed siren code is checked, and if it represents a dash, the TSIREN time variable is set to 720 milliseconds (step 532). Otherwise TSIREN is set to 240 milliseconds for a "dot." Operation then returns to step 520 (FIG. 10A).

The first step 540 of the ONSOUND routine (FIG. 10D) is to turn on the siren. The current siren code bit is checked, and if it represents a "dash," TSIREN is set to 720 milliseconds. Otherwise TSIREN is set to 240 milliseconds. Operation then returns (step 543) to step 520.

The SIREN subroutine therefore results in generation of the programmed personalized siren code at the appropriate time.

FIG. 10E shows the BURGLAR-BURGLAR subroutine 512B in further detail. If this feature is not enabled (during a programming mode), then operation immediately returns to the ALARM routine. If enabled, then a decision is made as to whether a sensor was just tripped (step 546A). If so, then the BURGLAR-BURGLAR timer is started (step 546B), and operation returns to the ALARM routine. In this embodiment, the timer has a duration of ninety seconds. If a sensor was not just tripped, then the timer is checked at step 547A, and if it has timed out to zero, operation returns to the ALARM subroutine. If the timer has not timed out, then at step 547B, the triggers are checked to determine if any trigger is active. If both conditions are true, then the BURGLAR-BURGLAR siren is turned

12

on for the alarm cycle duration, and operation returns to the ALARM subroutine.

The foregoing operation of the ALARM routine results in the system activating a first alarm device (e.g., siren 92) the first time a sensor device (e.g., a vibration sensor) become active. This starts the BURGLAR-BURGLAR timer. If a trigger also becomes active within the timer interval, then the BURGLAR-BURGLAR alarm device 91 is activated for the alarm cycle duration. As described above, the alarm device 91 may comprise a voice synthesizer for synthesizing the voice message "BURGLAR-BURGLAR" which may be alternated with a siren noise during the alarm duration. Thus, the user is clearly warned by a distinctive alarm indication that the second alarm event is an actual intrusion attempt, and not just a vibration sensor being set off.

The INT LIGHT subroutine is illustrated in FIG. 10F. When this feature is enabled by the installer of the system in the vehicle, the PULSATE INT LIGHT flag is set. The status of this flag checked at step 549B, and if it is not set, indicating that the feature has not been enabled, the controller 70 turns the interior light on for the duration of the alarm cycle (step 549B). If the PULSATE INT LIGHT flag is set, then the controller 70 pulsates the interior light on and off during the alarm cycle (step 549C). The controller 70 performs this function by alternatively changing the state of the output line 223 (FIG. 3) between the active and inactive states.

The CONTROL module is described in further detail with respect to FIGS. 11A-11D. At step 550 (FIG. 12A) the decoder is tested to determine if it is in the active state (step 498 of FIG. 9B). If not in the active state, then there is no decoder activity for the CONTROL module to respond to, and the operation returns to the main loop. If the decoder is active, then if it was just activated since the prior pass through the main loop, the panic timer is started (2.5 seconds) at step 552, and at step 553 the ARMED flag is checked to determine whether the system is armed. If armed, the DISARM subroutine (FIG. 11B) is entered. Otherwise the ignition switch is checked for its status and if turned on, the control function is ended and operation returns to the main loop. If the ignition switch is not turned on, then the ARM subroutine (FIG. 11C) is entered. One function of the CONTROL module then is to perform active arming (subroutine 555) or disarming (subroutine 559) of the system in response to receipt of a proper transmitted code.

Upon completion of either the DISARM or ARM subroutines, the control function is ended, and operation returns to the main loop. If, at step 551, the decoder was not just deactivated, then at step 557 the panic timer status is checked, and if "0" the PANIC flag is set at step 1558. Operation then returns to the main loop.

Upon entry of the DISARM subroutine (FIG. 11B), if the tandem security mode has been selected (step 557), then the INSTANT flag is cleared (step 558), the tandem timer is reset (step 559), and operation returns. If the tandem security mode has not been selected, then at step 560 the ARMED flag is cleared. At step 561, the trigger and sensor flags are checked to determine whether any tampering has occurred during the ARMED mode. If none of these flags are set, then at step 562 the audible chirp counter is set to 1, and at step 565 the appropriate chirp(s) is sounded. If tampering is indicated, then at step 563 the chirp counter is set to 3, and at step 564, the point of intrusion indicated by the

5,157,375

13

particular active flag or flags is loaded into the LED register for display by the LED control function (step 420 of FIG. 7). Thus, the system will sound a first predetermined audible message (here, one chirp) if no tampering was detected, and a second predetermined audible message (here, three chirps) if tampering was indicated. Further, the point of intrusion will be indicated by the LED flash code generated during the LED CONTROL function.

After sounding the appropriate number of chirps by the SOUND CHIRPS subroutine (FIG. 11C), which indicate audibly that tampering has or has not been detected, then at step 566 the vehicle power door system is activated to unlock the vehicle doors, the dome light is turned on (step 567) and operation returns to the main loop. Thus, upon disarming the system the vehicle doors are automatically unlocked, and the vehicle dome light is activated for a predetermined time interval or until the ignition switch is activated.

The SOUND CHIRPS subroutine is shown in FIG. 11C. If the system is determined to be in the PROGRAM mode (step 568A), then one chirp is sounded (step 569A), the chirp counter is decremented (step 569B) and the operation returns if the chirp counter state is zero, or otherwise loops back to step 569A. If the system is not in the PROGRAM mode, and if the CHIRP ENABLE flag is not set (step 568B), operation returns. If the flag is set, then operation proceeds to step 569A.

Upon entry of the ARM subroutine (FIG. 11D), at step 570, the SENSOR TEST and DOOR OK flags are cleared. At step 570A the controller 70 gets the trigger and sensor inputs, i.e., checks the various flags corresponding to these devices, and at step 571 determines whether the "HI/LO" feature has been disabled. If so, then operation branches to step 573. Otherwise, the status of the door trigger is ignored (step 572), and at step 573 the other trigger and sensor flags are checked to determine whether any of these other devices are active. If none are active, then at step 576, the chirp count is set to 2. Otherwise the active devices are disabled (step 574), to allow the system to be armed without the disabled sensor or trigger. This disabling takes place by storing the disabled sensor or trigger device identification, and thereafter ignoring the state of these identified devices each time the sensor and trigger lines are interrogated by the controller 70. At step 575 the chirp count is set to 4 indicating that a defective device has been bypassed. At step 577 the ARMED and INSTANT flags are set and the ENTRY DELAY flag is cleared. At step 578 the appropriate number of chirps is sounded, and at step 579 the door lock output line is activated to automatically lock the vehicle doors. Thus, the system automatically activates the door power locking system when the system is armed. Operation then returns to the main loop.

It will be appreciated that the purpose of the "HI/LO" feature is to allow the system to be actively armed even though the door trigger, which is assumed to be wired by the system installer to the vehicle interior light, is active. For vehicles with an interior courtesy light feature, wherein the light remains on for a predetermined interval after the door is closed, then the door trigger (node 201, FIG. 3) will remain active for some predetermined interval after the door is actually closed. Although the door triggers are initially ignored by the controller 70 (step 572) when the system is armed, the other triggers and sensors do provide some

14

security protection immediately. And once the door trigger (interior light) state becomes inactive after the courtesy light interval expires, the system senses this condition, and the door trigger state is automatically no longer ignored by the controller 70 so that the security system will trigger an alarm based on unauthorized door entry.

The DISARMED module (step 416 of FIG. 7) is shown in more detail in FIGS. 12A-E. At step 581, the HOOD subroutine (FIG. 12B) is entered. At step 582, the ignition switch is checked. If it is activated, then the SENSOR TEST flag is cleared (step 582A), and at step 583, a test is performed to determine whether the ignition switch was activated since the last pass through the subroutine. If so, the door lock system will be activated to lock the doors (step 585) if the auto lock feature has been enabled during the program mode (step 584). If the ignition switch was not just turned on or the auto lock feature is not enabled, the door lock step is bypassed. At step 583, the PROGRAM QUALIFY subroutine is entered which begins a 10 second timer after the ignition switch is turned on, during which interval the ENTER PROG module (step 426 of FIG. 7) can be entered by toggling the "valet" switch 77. At step 587 the EXIT DELAY flag is cleared, ending the exit delay during which the user is provided the opportunity to exit the vehicle without activating the alarm. Operation then returns to the main loop.

If the ignition switch was not on at step 582, a test is performed to determine whether the ignition switch was just turned off (step 588A). If so, then the doors will be unlocked (step 588C) if the auto lock feature is enabled. The valet flag is checked at step 588, and if set, the operation proceeds to step 587 to clear the EXIT DELAY flag. Otherwise, the SENSOR TEST flag is checked (step 589A) and if it was set during the installer program mode as described below, the status of each of the system sensors is checked. If none are active, the EXIT DELAY flag is cleared (step 589D), and operation returns to the main loop. If any sensor is active, the system sounds an appropriate number of audible chirps to identify the active sensor at step 589C. For example, assume the system comprises a vibration sensor and a glass breakage sensor, whose outputs are respectively connected to nodes 202 and 203 (FIG. 3) for interrogation by the controller 70. If only the vibration sensor is active, one chirp is sounded. If only the glass breakage sensor is active, two chirps are sounded. If both sensors are active, three chirps are sounded. The sensor test feature provides the installer the opportunity to test the installed system sensors after the system is installed, without putting the system in an armed mode and setting off the alarm siren device during the sensor testing for the alarm cycle duration. As a result, noise pollution is avoided. To use the feature, the SENSOR TEST flag is set by the installer enabling the feature during the installer program mode, as described in connection with the programming mode. Upon exiting the program mode, the system will loop through the functions of the main loop (FIG. 7), and will enter the DISARMED function (FIG. 12A). If the SENSOR TEST flag has not been cleared by arming the system with the remote transmitter (FIG. 11D) or by turning on the ignition (steps 582, 582A), the steps 589A-D will be repetitively performed as the system cycles through the main loop. The passive arming routine (step 596) will be bypassed. Thus, the installer may test the sensor operation by kicking the vehicle tires, tapping on the vehicle glass,

15

and the like to attempt to activate the sensors. If the sensors do not activate, a problem is indicated. This sensor test mode is exited by actively arming the system or by turning on the vehicle ignition.

The passive arming flag is checked at step 590, and if this feature is disabled, operation proceeds to step 587. If the passive arming feature is not disabled, then at step 592 the RECORD subroutine is called. At step 594, the door triggers are tested to determine whether a door has been opened and closed. If not, then the determination is made (step 595) as to whether the ignition switch has been turned on since the system was disarmed. If it has, then the PASSIVE routine (596) is bypassed, this indicating that passive arming of the system should not occur. At step 598, the UPDATE subroutine is called.

The HOOD subroutine is shown in FIG. 12B. At step 600, the status of the "hood" program switch (one of switches 77) is interrogated to determine whether the hood switch was just activated since the last pass through the subroutine. If yes, then the status of the hood release controlled device 96 is checked to see whether it is active (step 601). If active, it is turned off (step 602); if not active, the hood release device is turned on (step 603). Operation then returns. If the hood switch was not just activated (step 600), operation returns via step 604 if the hood release device is not active. If the hood release is active (step 604), the hood sensor is checked (step 605), and if open, operation returns. If not open, the determination is made at step 606 if the hood was closed since the last pass through the subroutine. If it was, a 30-second timer is started, and operation returns. If not, then at step 607, the 30-second timer is checked to determine whether it has timed out. If it is timed out, the hood release device is turned off, locking the hood, and operation then returns to step 582.

The RECORD subroutine is shown in FIG. 12C. The purpose of this routine is to record in the trigger/sensor register comprising the controller 70 any active triggers or sensors. Thus, at step 610, the ignition switch is checked to determine whether it was turned off since the last pass through the subroutine. If not, then operation returns. If the ignition switch was just turned off, the contents of the trigger/sensor register maintained by the controller are accessed (step 611), and the door triggers are ignored at step 612. Then any active sensor or triggers, excepting the door triggers, are recorded in the register (step 613). Operation then returns to step 594.

In the PASSIVE subroutine (FIG. 12D), the system is passively armed, if the conditions are appropriate. The exit delay timer is checked at step 620 to determine whether the exit delay is over. If it is, then at step 621, any triggers or sensors recorded in the trigger/sensor register as being active (step 613) are disabled, and at step 622 the ARM flag is set. A determination is made (step 623) as to whether the door was opened during the disarmed mode. If so, operation returns to the main loop. If not, the door lock device 94 is activated to lock the doors (step 624). If the exit delay is not over (step 620), then at step 625 the contents of the trigger/sensor register are fetched, and at step 626 the contents of the "record" register, i.e., those active triggers and sensors recorded at step 612 (FIG. 12C), are masked from the trigger/sensor register contents. If the result is a blank register, this indicates that there has been no change in the status of the triggers and sensors. If the result is not zero, a change has occurred in the status of the trig-

5,157,375

16

gers/sensors. The record register is updated (step 627A) to remove the trigger or sensor which is no longer active, so that that device is no longer disabled. The exit delay timer is then reset before returning (step 628).

The UPDATE subroutine is illustrated in FIG. 12E. The purpose of this subroutine is to clear any bit in the record register that is inactive as illustrated in steps 630 and 631 in FIG. 12E.

The ARMED function 414 (FIG. 7) is illustrated in FIGS. 13A-F. The first step 640 (FIG. 13A) of this function is to determine the status of the triggers and sensors. At step 642, any sensors or triggers previously identified as disabled are masked out. The next steps 643-46 are to execute the subroutines DOOR, ENTRY, SENSOR and OTHER TRIGS which are shown in FIGS. 13B-E, so as to determine which active trigger or sensor elements should result in activating the alarm controlled elements. At step 646A, the FACT subroutine (FIG. 13G) is called. At step 647, the TRIPPED flag is checked, and if set, the SHUT OFF subroutine (FIG. 13F) is executed. Otherwise, the trip counter is reset (step 649) to 10. The purpose of the trip counter is to prevent alarms from continuing after ten successive passes due to the same trigger or sensor being active. This prevents noise pollution and conserves the vehicle battery by limiting the alarm sounding due to a particular sensor or trigger to a predetermined cumulative activation interval equal to a given number of alarm cycles before the system is disarmed and rearmed. Operation then returns to the main loop.

Referring now to FIG. 13B, the DOOR subroutine is depicted. The door triggers are checked at step 651, and if not active (i.e., the doors are closed), then the DOOR OK flag is set (step 652) and operation proceeds to the ENTRY subroutine. If a door trigger is active, then if the "HI/LO" feature described above is not disabled (step 653), the DOOR OK flag is checked. If this flag is not set, operation proceeds to the ENTRY subroutine and the open door condition does not result in an alarm condition. If the "HI/LO" feature is disabled, or if the DOOR OK flag is set, then the INSTANT flag is checked (step 655), and if set, the door trigger active status is interpreted as an alarm condition, the TRIP flag is set (step 656A) and the intrusion point is recorded (step 656B) before proceeding to the ENTRY subroutine. If the INSTANT flag is not set, then at step 657A, the ENTRY DELAY flag is set, the dome light is turned on at step 657B, and the entry delay timer is started at step 657C. Thus, if the door trigger line is wired to the interior light and the vehicle has a courtesy light delay feature, the HI/LO feature of the system will not act on an active door trigger to declare an alarm event until after the door trigger becomes inactive (step 651) and the DOOR OK flag is set. The system provides full intrusion protection as soon as the door trigger becomes inactive, in contrast to conventional systems having a fixed predetermined time delay during which the status of the door trigger is ignored for purposes of declaring an alarm event.

The ENTRY subroutine is shown in FIG. 13C. The ENTRY DELAY flag is checked (step 658), and if not set, operation proceeds to the SENSOR subroutine. If the flag is set and if the entry delay timer state is "0," then the TRIPPED flag will be set. Operation otherwise proceeds to the SENSOR subroutine.

The first step 661 of the SENSOR subroutine (FIG. 13D) is to check the five-second timer initiated when the system was armed. If the timer has not timed out,

the sensor lines or bits are masked out (step 662) and operation proceeds to the OTHER TRIGS subroutine (FIG. 13E). If the timer has reached zero, then the sensor lines are checked (step 663), and if none are active, operation proceeds to the OTHER TRIGS subroutine. If a sensor is active, the TRIPPED flag is set (step 664), and operation proceeds to the OTHER TRIGS subroutine.

In the OTHER TRIGS subroutine (FIG. 13D), the triggers other than the door triggers are checked. If none are active, operation proceeds to step 647 (FIG. 13A). If any other triggers are active, the TRIPPED flag is set at step 668, and operation proceeds to step 647.

The SHUTOFF subroutine (FIG. 13F) is entered if the TRIPPED flag has been set. Here, the trip counter is decremented (step 672) and if its state is not zero, the intrusion point is recorded (step 674), and operation returns to the main loop. If the trip counter has reached zero, it is reset (step 675), the intrusion point trigger or sensor is disabled, and operation returns to the main loop. Thus, once the trip counter reaches its zero state, an alarm will not be generated as a result of the active trigger or sensor device on the next pass through the main loop.

FIG. 13G shows the FACT (false alarm control and test) subroutine, whose function is to minimize false alarms due to repetitive sensor triggering. The first time a sensor is triggered, an alarm condition will be declared without regard to the status of the trigger devices. But, if the FACT feature is enabled, once a sensor has tripped an alarm (i.e., since the system was armed), then subsequently (until the system is disarmed), an active sensor condition will cause an alarm only if another trigger is also active. Thus, if at step 678A, the FACT feature has not been enabled, operation immediately returns, with the result that a sensor active signal will trip an alarm. If FACT is enabled, then the sensors are checked to find any active sensors (step 678B). If none are active, operation immediately returns. If a sensor is active, and if the system has not previously been tripped by this sensor (step 678C), the TRIP flag is set (step 679) and operation returns. If the system has previously been tripped, operation will return without setting the trip flag unless another trigger is active (step 678D).

The LED CONTROL function (step 420 of FIG. 7) is shown in further detail in FIGS. 14A-C. At step 680 (FIG. 14A), the ARMED flag is checked to determine whether the system is in the armed mode. If not armed, the IDENTIFY subroutine is entered at step 681. Otherwise, the DIAGNOSE subroutine is entered at step 682 and thereafter operation returns to the main loop.

The IDENTIFY subroutine is shown in FIG. 14B. At step 686, the controller determines whether an intrusion was attempted while the system was armed. If not, then the green LED is flashed (step 689) and operation returns to the main loop. If an intrusion was attempted, then at step 687, the message counter is checked, and if zero, the INTRUSION flag is cleared (step 689), the green LED is flashed, and operation returns to the main loop. If the counter is not zero, then it is decremented (step 690). At step 691 the point of intrusion is established by reading the flags associated with the activated triggers and sensors stored in the register. The proper LED pulse count corresponding to the intrusion point is set (step 692), and at step 693, the appropriate LEDs are turned on. At step 694 the voice synthesizer is activated

to announce audibly the intrusion point. It will be appreciated that the voice synthesizer is programmed to provide a plurality of messages, and that a particular message may be chosen and activated in correspondence to a particular control signal from the controller 70. Such a selection may be accomplished by a look-up table function, as where a particular intrusion point code selects the appropriate message. Voice synthesizers are known in the art having the capability of generating a selected one of a plurality of stored messages. Operation then returns to the main loop.

The DIAGNOSE subroutine is shown in FIG. 14C. At step 695, the controller determines whether there is a disabled trigger or sensor. If not, at step 696, a red LED is flashed, and operation then returns to the main loop. If a sensor or trigger is disabled, then the message counter is checked (step 697), and if "0," the LED is flashed, and operation returns to zero. Otherwise, the counter is decremented (step 698), the data defining the disabled trigger or sensor is obtained (step 699), the proper pulse counter corresponding to the particular disabled sensor or trigger is set (step 700), and visible and audible messages identifying the disabled element are generated at steps 701 and 702 by the LED and voice synthesizer.

Conventional security systems may be provided with particular features that may be enabled or disabled for a particular vehicle installation. However, this enabling/disabling is conventionally performed by the system installer, by cutting wires, grounding pins, and the like. The system user has no ready means of reconfiguring the feature selection after the system is installed.

In accordance with another aspect of the invention, a programming means is provided for enabling or disabling particular system features which does not require the use of any tools and which may be used by the system user.

FIGS. 19A-L of the referenced U.S. Pat. No. 4,887,064, disclose one technique for selecting programming options when in the program mode. Reference is made to these figures and the description thereof in the pending patent application for further details regarding the specific functions which are programmed. As described there, the program switch is monitored to select a desired programming function by toggling the switch a predetermined number of times to select a particular function for programming data. When there are many possible programming options, and the data input device available to the user is a three position switch comprising the "program" and "valet" positions or switches, such a procedure can be inconvenient to the user. In accordance with the invention, the user-programmable functions are grouped in several possible branches, and the user first selects a desired branch and then a desired function within the branch. This simplifies the selection of a desired function to be programmed. Further, certain programmable functions are grouped which are to be programmed only by the system installer, and not by the user, are grouped in a separate branch which is accessed by a different programming technique than the user-programmable functions.

FIG. 15A is a graphical depiction of the three program branches in the user program mode and the single branch in the installer program mode, for this embodiment. The particular number of branches and the number of programmable functions grouped in each branch will, of course, depend on the particular system imple-

mentation. The user program mode includes the branch for programming the "enable/disable" features, the branch for programming the siren control features, and the branch for programming the remote control features. The first branch includes here three possible features, the sensor programming function, the automatic lock enable/disable, and the passive arming enable/disable. The siren control branch includes four possible functions, the FACT enable/disable, the siren and entry delay duration selection, the personalized siren programming and the chirp enable/disable functions. The remote control branch includes three remote control programmable functions.

The installer program mode branch includes five functions, programmable door trigger polarity, the BURGLAR-BURGLAR feature enable/disable and the door lock control signal duration feature, the sensor test feature and the interior light pulsation feature.

Both the user and installer programming mode are entered using the same three-position switch, which has an off position, a latched-on position (the valet switch or position) and a momentary-on, spring-loaded-toward-the-off position (the program switch or position). However, the user mode is entered by, within ten seconds of turning the ignition switch on, holding the program switch on until a chirp is heard. A branch must be selected within one minute, by toggling the program switch once, twice or three times, to select the first second or third programming function in this branch as desired, and then toggling the valet switch to the on position and then off to enter this data. The system will sound the same number of long chirps as the number of the function selected in this manner. Then once a branch has been selected, a particular function within the selected branch must be selected within one minute by the same procedure, i.e., by toggling the position switch the same number of times as the preset reference number associated with the desired function, and entering this data by toggling the valet switch. The system will provide short acknowledgement chirps indicating the function selected.

To enter the installer program mode the program switch is toggled three times to the on position within ten seconds of the ignition switch being turned on. The system will sound three chirps indicating that the installer programmable mode has been selected. The desired function within this program branch is then selected in the same manner as described above with respect to the user programmable function selection once a branch has been selected.

The ENTER PROG function (step 426 of FIG. 7) is shown in further detail in FIGS. 15A-U. At step 705, the 5 second program qualify timer (started at step 586, FIG. 12A) is checked. If its state has reached "0," operation returns to the main loop. If the counter has not reached "0," then the program switch 77 is checked at step 706 to determine if it is being held to the on position. If so then the user program mode is called at step 707. If the program switch is not being held on, then if the program switch has been toggled three times at step 708, the installer program mode is entered at step 709.

The user programmable mode branch selection is shown in FIG. 15C, where at step 710 the system sounds the acknowledgement chirp indicating that the user program mode has been entered as described above. Steps 711, 713 and 715 indicated decisions as to whether the enable/disable feature branch (branch 1), the siren control branch (branch 2) or the remote con-

trol branch (branch 3) was selected by the user. The selected branch is called at corresponding steps 712, 714 and 716. Upon return from the branch acknowledgement chirps are sounded if the user branch programming is completed (steps 717 and 718).

FIG. 15D represents the function 712 (FIG. 15), showing the selection of a particular function within the enable/disable branch. Thus, at step 720 an appropriate number of chirps is sounded, one chirp for branch 1, and at steps 721, 724 and 727 the program/valet switch is monitored to determine when a particular function is selected for programming. If the programmable sensor function is selected (step 721), then the acknowledgement chirp for this selection, here one chirp, is sounded and the PROG SENSOR routine is called. If the automatic locking enable/disable feature is selected (step 724), then two chirps are sounded (step 725) and the PROG AUTO LOCK routine is called (step 726). If the passive arming enable/disable feature is selected (step 727), then three chirps are sounded (step 728) and the PROG AUTO ARM routine is called (step 729).

FIGS. 15E-G illustrate the PROG AUTO ARM, PROG SENSOR and PROG AUTO LOCK routines respectively. For example, the PROGRAM AUTO ARM routine commences with the sounding of a single chirp as an acknowledgement that this routine has been selected (step 730). At step 731, the program switch 77 is checked and if on, the passive arming feature is disabled (step 732). If the program switch is not on, then the valet switch is checked (step 733) and if on, the passive arming feature is enabled (step 734). The PROG SENSOR routine and the PROG AUTO LOCK routines operate in a similar manner. The purpose of the PROG SENSOR routine is to put a programmable sensor device in its program mode for programming its sensitivity to vibration and shock. Such a sensor is described in the patent application entitled "Programmable Sensor Apparatus," Ser. No. 07/230,260, filed Aug. 9, 1988, by Ze'ev Drori and Moti Segal, U.S. Pat. No. 4,845,464.

FIG. 15H shows a flow chart of the siren control branch selection, which operates in a similar fashion to the enable/disable feature branch selection shown in FIG. 15D. The features which are programmed through this branch are FACT (FIG. 15I), the entry delay and siren duration feature (FIG. 15J), the personalized siren tone (FIGS. 15K and L) and the chirp enable/disable (FIG. 15M).

The FACT feature has been described above with respect to FIG. 13G. As illustrated in FIG. 15I, the user may enable or disable this feature during the user programming mode.

FIG. 15J illustrates the user programming of the entry delay and the alarm siren cycle duration. This feature allows the user to program the desired entry delay and siren duration.

FIG. 15K illustrates the SIREN TONE routine, the personalized siren programming feature, wherein the user can personalize the particular siren sound by programming a siren sound to comprise a series of "dots" and "dashes." FIG. 15L shows the PROG CHIRP routine, which permits the user to disable the sounding of chirps normally indicating the arming or disarming of the system. These features are described more fully in U.S. Pat. No. 4,887,065.

The programming feature selection for the third branch, the remote control branch, is shown in FIG. 15N. There are three functions in this branch, all involv-

ing the programming in the system controller memory of remote transmitter codes, as described in pending patent application entitled "Electronically Programmable Remote Control Access Systems," Ser. No. 07/094,395. In this embodiment there are four channels, each of which may be programmed to be responsive to a plurality of transmitter codes for performing a given function. For example, channel 1 arms and disarms the system. Channels 2-4 may be used for other purposes, such as to open the trunk lid remotely, and the like. The routines PROG CH1/CH2, PROG CH3/CH4, and PROG CH3+CH4 are shown in FIGS. 150-15Q. Thus, FIG. 150 shows the selective programming of a particular code for either channel 1 or 2, FIG. 15P the selective programming of a particular code for either channel 3 or 4, and FIG. 15Q shows the selective programming of codes under either channel 3 or 4 to actuate channel 3 (to allow more codes to entered for channel 3.)

FIG. 15R shows the selection process for selecting the features to be programmed in the installer program mode. There are five features, the door trigger polarity routine (FIG. 15S), the BURGLAR-BURGLAR routine (FIG. 15T), the door lock pulse duration routine (FIG. 15U), the sensor test feature and the interior light pulsating feature (FIG. 15V).

The door trigger polarity (active high or low) for the particular vehicle is programmed by the installer by opening the vehicle door and selecting this feature for programming. By setting or clearing the POS DOOR flag automatically, the system is programmed to respond to the appropriate door trigger polarity.

FIG. 15T shows the selective enabling or disabling of the BURGLAR-BURGLAR feature by the installer. FIG. 15U allows the installer to select either a standard (typically) one-second output pulse duration for activating the vehicle power door locking and unlocking, or a long pulse duration (typically 3 seconds) for vehicles employing a door locking system requiring such longer length pulses.

From the foregoing, it is apparent that the various features of the system may be easily accessed during the program mode to enable, disable or program the various features of the system described above. For example, say that the user wishes to access the "auto arm" feature. After entering the user program mode, the user simply enters "1" to select branch 1, and then enters "3" to select the "auto arm" feature. The user then puts the switch 77 to the valet position to enable this feature. The preassigned number designations for the branches and features within each branch may typically be set forth in a user's manual accompanying the system. The manner in which the installer program mode is selected, as well as the features selectable in this mode, may be described in an installation manual which need not be given to the system user.

FIG. 15V allows the installer to enable or disable the interior light pulsate feature, wherein the interior light is cycled on and off during an alarm cycle.

Upon completion of the program mode, operation returns to the the main loop.

The BATTERY CHECK function module is shown in FIG. 16. This module prevents the system from draining the battery when an alarm condition is detected. The DOME LIGHT function module is shown in FIG. 21. The purpose of this module is to provide the capability of turning the vehicle courtesy light on and leaving it on for a predetermined period of time after

the system has been disarmed, or until the ignition switch is turned on. The next function performed during the main loop (FIG. 7) is the ENGINE CONTROL function (step 434), shown more fully in FIG. 18. This function allows the vehicle engine to be disabled from unauthorized starting. Each of these functions is described more fully in the referenced U.S. Pat. No. 4,887,064.

Referring now to FIG. 19, the output protection circuitry comprising the invention is shown. FIG. 19 is a simplified form of FIG. 3, with many of its elements omitted for the sake of simplicity and clarity of description of this facet of the invention. Thus, the system includes a microcomputer 70' which receives sensor and trigger data at terminals P1'-Pn'. The microcomputer 70' controls a plurality of output devices by setting the states of output terminals P11'-P1n'. Thus, for example, terminal P11' may control an output circuit comprising FET transistor 236' which in turn drives the alarm siren through line 230'. Thus, the output P11' gates the FET transistor on or off. When the transistor is gated to the conductive state, the current through the drain to source regions of the FET is largely dependent on the impedance of the siren or other controlled device. If line 230' is inadvertently connected to +12 volts during installation and the transistor is gated on, a large destructive current will flow through the FET device, quickly resulting in damage to the device.

In accordance with the invention, a current sensing circuit is employed to provide a high current signal to the microcomputer 70' which acts on this information to turn off the output controlling the current handling element, thereby preventing damage to the FET. Thus, node X provides the potential difference between the FET drain and the source connection to chassis ground, V_{DS} . As is well known, the drain to source potential difference is a measure of the current flow through the device when the device is gated to the conductive state by an appropriate potential applied to the device gate connection, since there is some resistance in the device. The current sensing circuit generates a high current warning signal when the voltage V_{DS} exceeds a predetermined level.

As shown in FIG. 19, the potential at node X is coupled through resistor X1 and diode X3 to the base of transistor X4. Node X5 is connected to the transistor emitter and to a biasing resistor X2. Node X5 is at the logic ground for the system. A logic ground (L.G.) circuit is connected to the chassis ground plane and includes a pair of diodes connected in parallel but in opposite sense. As a result, the logic ground plane is at a potential one diode junction drop or about 0.6 volts above the chassis ground plane. Thus, with diode X3 in series between the node X and the gate of transistor X4, and with the emitter at a 0.6 volt potential above chassis ground or the potential of the FET source, a voltage V_{DS} level of at least about 1.2 volts is required to gate the comparator transistor X5 to the conductive state. With terminal L of the microcomputer 70' connected to the collector of transistor X5, an active low state of the terminal L will indicated the high current condition.

The microcomputer 70' periodically and frequently checks the status of the current sense terminals including terminal L, when call the routine OUTPUT PROTECTION in the main loop (FIG. 7) and when an active signal is sensed, the corresponding output terminal, here P11' is turned off, thereby preventing permanent damage to the output device 246'.

23

It will be appreciated that other current sensing circuits may be employed to achieve the function, e.g., with output devices other than FETs.

It is understood that the above-described embodiments are merely illustrative of the possible specific embodiments which may represent principles of the present invention. Other arrangements may readily be devised in accordance with these principles by those skilled in the art without departing from the scope of the invention.

What is claimed is:

1. A vehicle security system comprising means for detecting attempted intrusions to a vehicle when the system is put into the armed mode, means responsive to indications of a detected intrusion for activating an audible signal generating device for a predetermined alarm cycle duration, said means responsive to indications of a detected intrusion resetting after expiration of said duration so as to be activated again in the event of another intrusion after the first of said detected intrusions, and means for disabling, until said system has been disarmed and rearmed, further operation of said audible signal generating device in response to indications of a detected intrusion from said detecting means after said audible signal generating device has been activated by said detecting means a predetermined cumulative time interval after the system has been put into the armed mode, said cumulative time interval being longer than said alarm cycle duration, thereby reducing the noise pollution which might otherwise be created by a repetitive alarm condition.

2. The system of claim 1 wherein said predetermined time interval is the time duration of a predetermined number of successive alarm cycles.

3. A vehicle security system which does not continuously cycle through alarm cycles due to a constantly or repetitively active sensor or trigger device, comprising: at least one sensor or trigger device for sensing an intrusion event and providing a device activated signal when the event is detected;

means for generating audible alarm alert signals in response to appropriate alert control signals;

a controller for controlling the operation of said security system so that said system may be operated in an armed mode wherein said controller monitors said at least one sensor or trigger device and generates the appropriate alert control signals to cause said audible alert generating means to issue an audible alarm alert signal of an alarm cycle duration in response to said device activated signal, or in a disarmed mode wherein said system is disabled from generating said alarm alert signals, said controller comprising:

means for monitoring the number of alarm cycles activated since the system was placed in the armed mode and preventing said audible alert generating means from activating further audible alarm alert signals after said number exceeds a predetermined number;

wherein said means for preventing said audible alert generating means from activating further audible alarm alert signals comprises means for monitoring the number of consecutive times one of said sensor or trigger devices is tripped and disabling said sensor or trigger device from thereafter activating said means for activating the audible alert generating means, without disabling the other of said sensor or trigger devices from thereafter activating

5,157,375

24

said means for activating the audible alert generating means.

4. The system of claim 3 wherein said at least one sensor or trigger device includes a door trigger for generating a trigger device active signal when a door is open, whereby a continuous defect in said trigger, or the leaving of said door open, will, after activating said audible alert generating means said predetermined number of alarm cycles, no longer result in activation of said audible alert generating means, thereby minimizing noise pollution which would otherwise result from further activation and conserving battery power of the vehicle.

5. The system of claim 3 wherein said at least one sensor or trigger device includes a vibration sensor device, whereby repeated activations of the vibration sensor device will, after activating said audible alert generating means said predetermined number of alarm cycles, no longer result in activation of said audible alert generating means, thereby reducing the attendant noise pollution and conserving battery power of the vehicle.

6. The system of claim 3 wherein said at least one sensor or trigger device comprises:

a sensor device for sensing an intrusion event and providing a sensor device activated signal when said event is detected; and

a trigger device for indicating the open/close status of one or more of the vehicle's accessible compartments and providing a trigger device activated signal when said one or more compartments are open;

wherein said controller generates said appropriate alert control signals in response to either said sensor device activated signal or said trigger device activated signal; and

wherein said means for preventing said audible alert generating means from activating further audible alarm alert signals comprises means for monitoring the number of consecutive times one of said sensor or trigger devices is tripped and disabling said sensor or trigger device from thereafter activating said means for activating the audible alert generating means, without disabling the other of said sensor or trigger devices from thereafter activating said means for activating the audible alert generating means.

7. A vehicle security system which may be armed or disarmed by a remote control transmitter, and which is operable to automatically rearm the system a predetermined time interval after disarming by remote control if none of the vehicle doors has been opened, comprising:

vehicle antitheft means;

a remote control transmitter for generating an encoded signal;

means operable when the system is armed and responsive to receipt of said encoded signal for disarming said system; and

means for automatically rearming said system in the event none of the vehicle doors is opened during a time interval of predetermined length after said system is disarmed by said remote control transmitter.

8. The system of claim 7 wherein said means responsive to receipt of said encoded signal for disarming said system further comprises means for automatically unlocking one or more of the vehicle doors, and said means for automatically rearming said system further comprises means for automatically locking said one or

more vehicle doors when said system is automatically rearmed.

9. The system of claim 8 wherein said system further comprises means for arming said system in response to receipt of said encoded signal generated by said transmitter, and means for locking one or more of the vehicle doors when the system is armed in response to receipt of said encoded signal.

10. The system of claim 9 wherein receipt of said encoded signal when the system is in the disarmed state results in the arming of the system, and wherein receipt of said encoded signal when the system is in the armed state results in the disarming of the system.

11. The system of claim 8 wherein said system further comprises means for arming said system in response to receipt of a second encoded signal generated by said transmitter, and means for locking one or more of the vehicle doors when the system is armed in response to receipt of said second encoded signal.

12. A vehicle security system, comprising:

- at least one sensor device for sensing attempted tampering with said vehicle and generating a "sensor active" signal when the sensor device is tripped;
- at least one trigger device for monitoring the open/closed status of one or more of the vehicle access locations, and providing a "trigger active" signal when said location has an opened status;
- a first alert means for generating a first type of alarm alert signal in response to a first alarm event signal;

a second alert means for generating a second type of alarm alert signal in response to a second alarm event signal;

means for selectively arming or disarming said security system; and

an electronic controller for controlling the operation of said security system, said controller responsive to said "sensor active" and "trigger active" signals while said system is armed for generating said first and second alarm event signals under predetermined conditions, said controller comprising:

means responsive to receipt of the first said "sensor active" signal after said system is armed for activating said first alert means to generate said first type of alert signal for a limited time duration;

means responsive to at least said first "sensor active" signal after said system is armed for activating said second alert means for a limited time duration if said "trigger active" signal is generated within a predetermined time interval after receipt of said first "sensor active" signal.

13. The security system of claim 12 wherein said first alert means comprises a siren.

14. The security system of claim 12 wherein said second alert means comprises means for generating a voice synthesized message.

15. The security system of claim 12 wherein said controller further comprises means for bypassing said sensor device after receipt of said first "sensor active" signal so that second and subsequent receipts of said "sensor active" signal do not result inactivation of said first alert means.

* * * * *

35

40

45

50

55

60

65



US005534845A

United States Patent [19]

[11] **Patent Number:** 5,534,845

Issa et al.

[45] **Date of Patent:** Jul. 9, 1996

[54] **ADVANCED AUTOMOTIVE AUTOMATION AND SECURITY SYSTEM**

4,885,572	12/1989	Iwata et al.	340/425.5
4,987,402	1/1991	Nykerk	340/426
5,146,215	9/1992	Drori	340/426
5,153,558	10/1992	Robinson et al.	340/426
5,216,407	6/1993	Hwang	340/426

[76] **Inventors:** Darrell E. Issa, 1598 Parkview Dr.;
 Jerry W. Birchfield, 743 Imperial Dr.;
 Glenn R. Busse, 2130 Redwood Crest;
 Sidney B. Perdue, 820 Sycamore Ave.,
 #200, all of Vista, Calif. 92083;
 Kenneth A. Ward, 3622 Mary La.,
 Escondido, Calif. 92025

Primary Examiner—John K. Peng
Assistant Examiner—Nina Tong
Attorney, Agent, or Firm—John J. Murphey; Murphey Law Offices

[57] **ABSTRACT**

An electrically powered security system for monitoring and controlling access to a protected area and having multiple levels of alert signal commensurate with the level of security threat to the area; a siren for communicating multiple levels of alert signal, both visual and audible, progressively including: a low level, medium level and full level alert consisting of a voice warnaway, a series of audible chirps, or blinking lights; an electrically erasable and programmable read only memory for permanently storing system operational parameters and a controller for using the operational parameters for controlling the operation of security system, the security system including a remote transmitter to remotely test all input sensors and remotely disable specific sensors from operation, thus having control of any combination of variable audio and/or audio-visual alarm response, the security system further including a light control for automatic light engagement and mutual cooperation with windshield wipers.

[21] **Appl. No.:** 945,667

[22] **Filed:** Sep. 16, 1992

[51] **Int. Cl.⁶** B60Q 1/00

[52] **U.S. Cl.** 340/425.5; 340/426; 340/457.2;
 340/460; 307/9.1; 307/10.2; 180/167

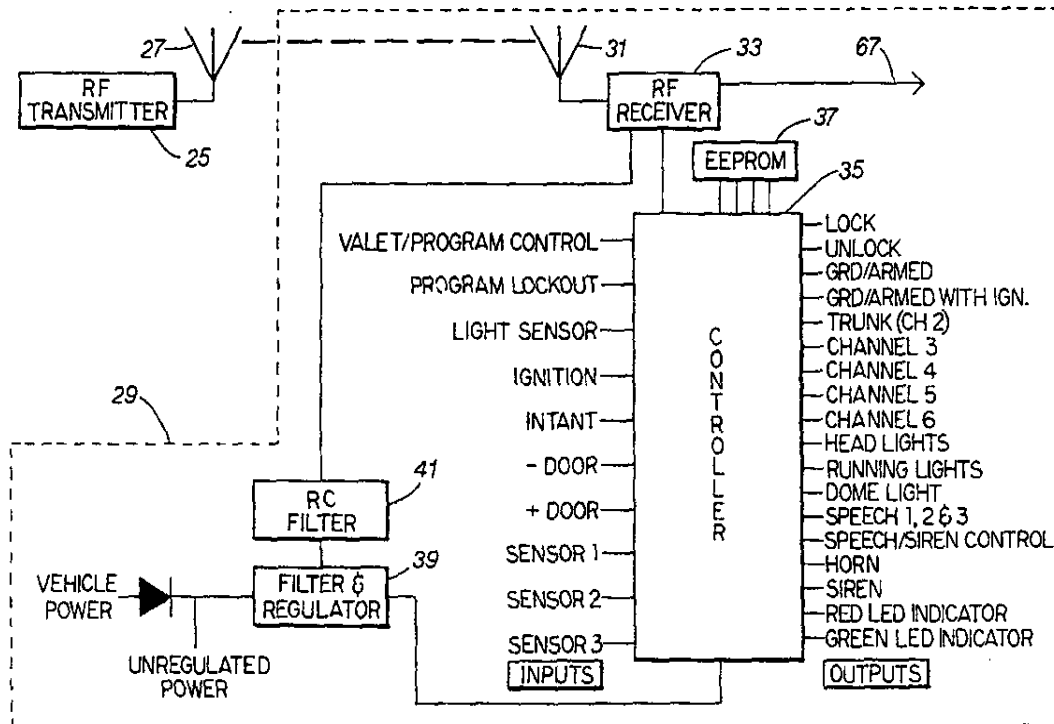
[58] **Field of Search** 340/425.5, 426,
 340/457.2, 469, 439, 460, 458, 430, 429,
 384 E, 384 R, 531, 541, 539, 561, 565,
 567, 551, 309.15; 307/9.1, 10.1, 10.2; 108/167

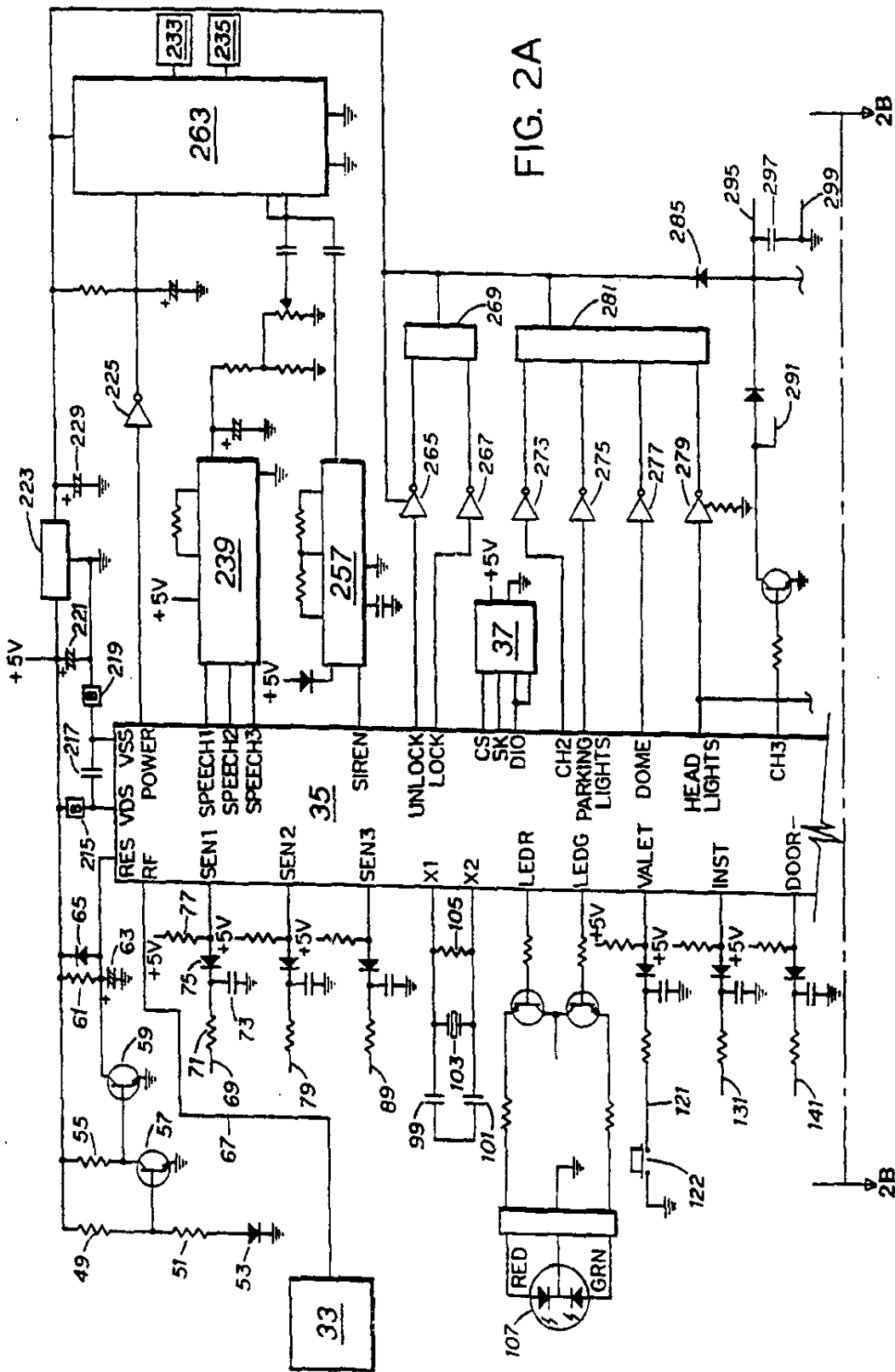
[56] **References Cited**

U.S. PATENT DOCUMENTS

4,045,769	8/1977	Faller	340/457.2
4,376,909	3/1983	Tagami et al.	340/457.2
4,674,454	6/1987	Phairr	180/167
4,719,775	1/1988	Pross et al.	70/264
4,754,255	6/1988	Sanders et al.	340/426
4,794,368	12/1988	Grossheim et al.	340/426

32 Claims, 23 Drawing Sheets





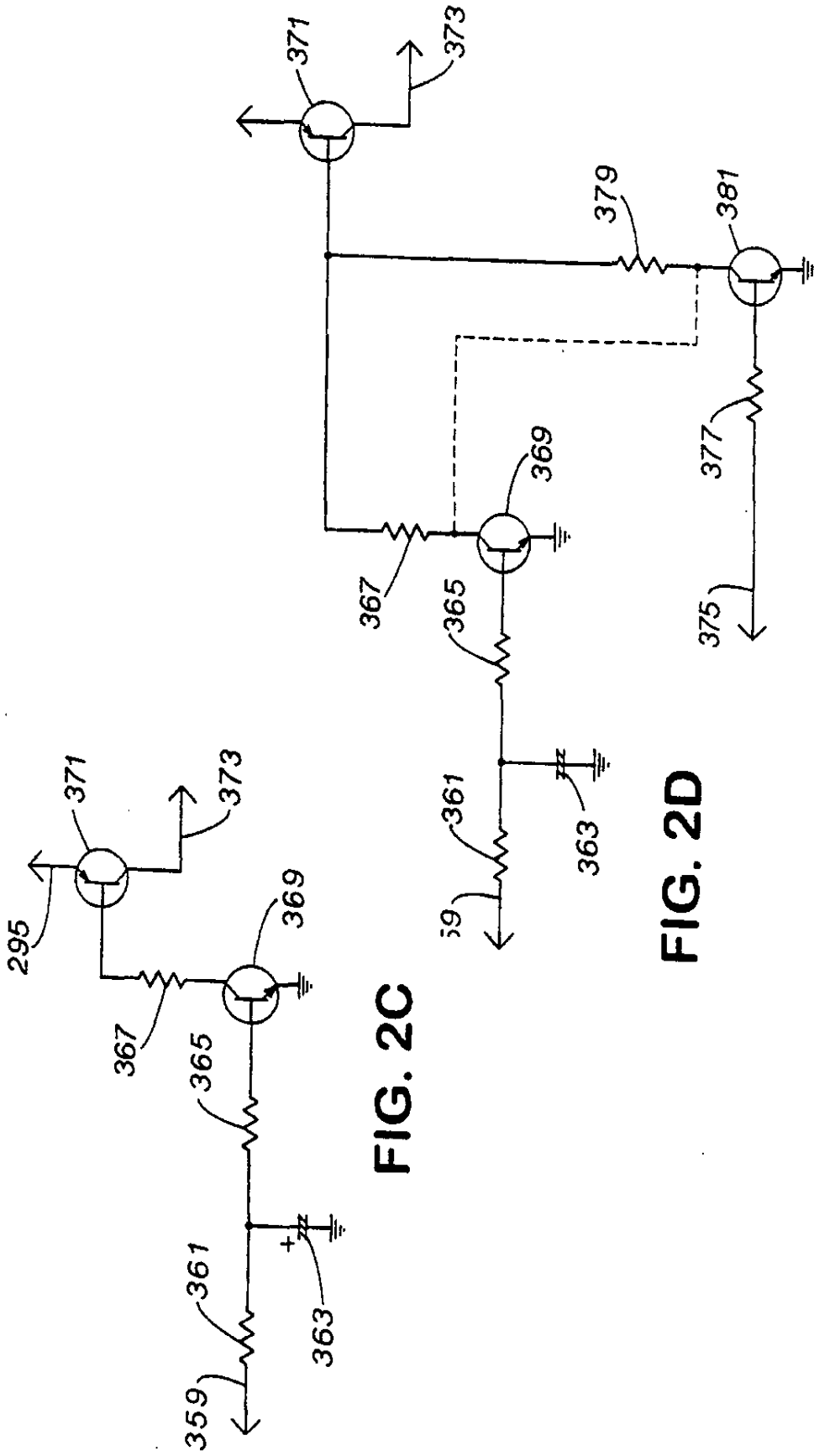


FIG. 2C

FIG. 2D

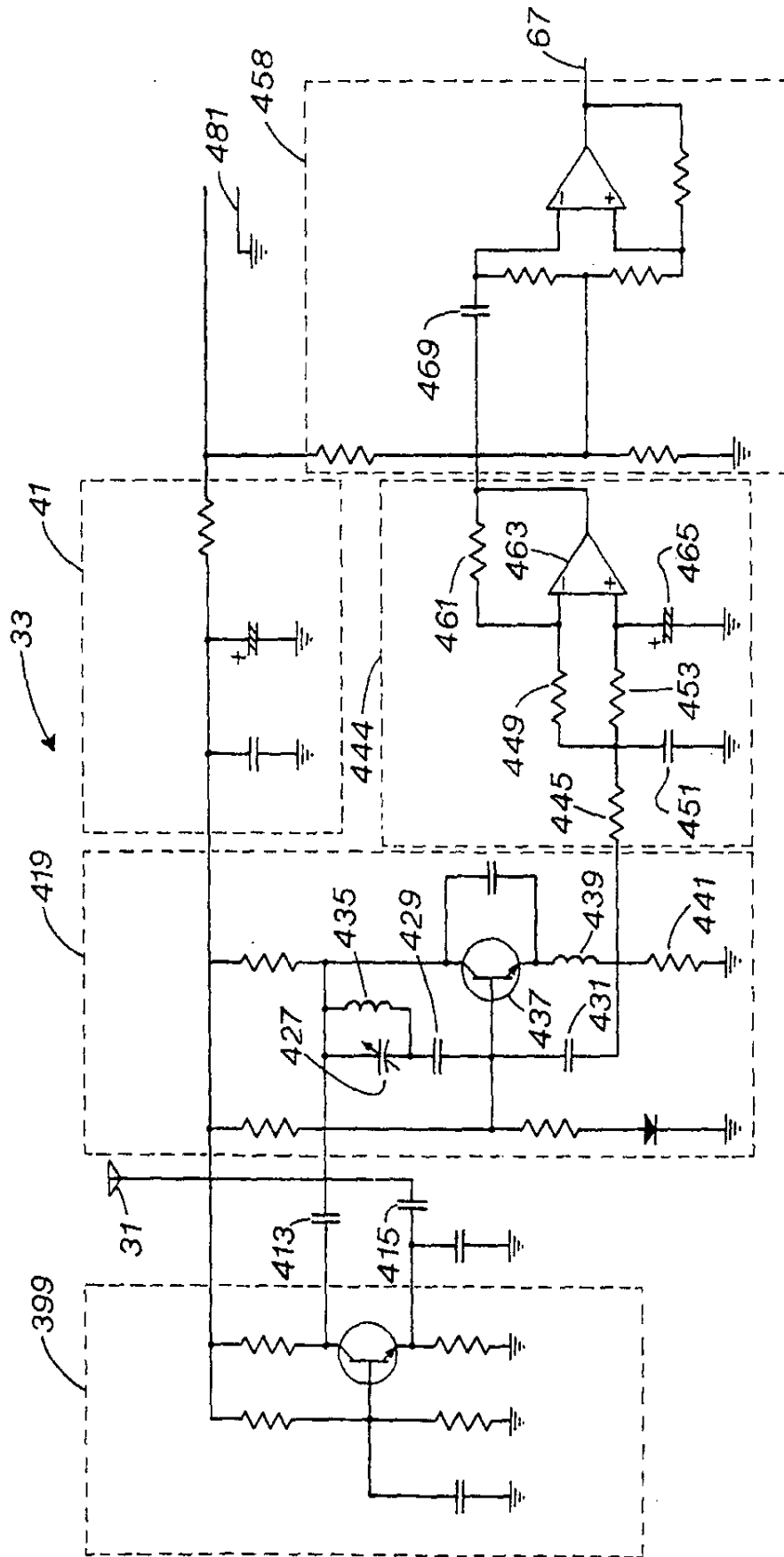


FIG. 3

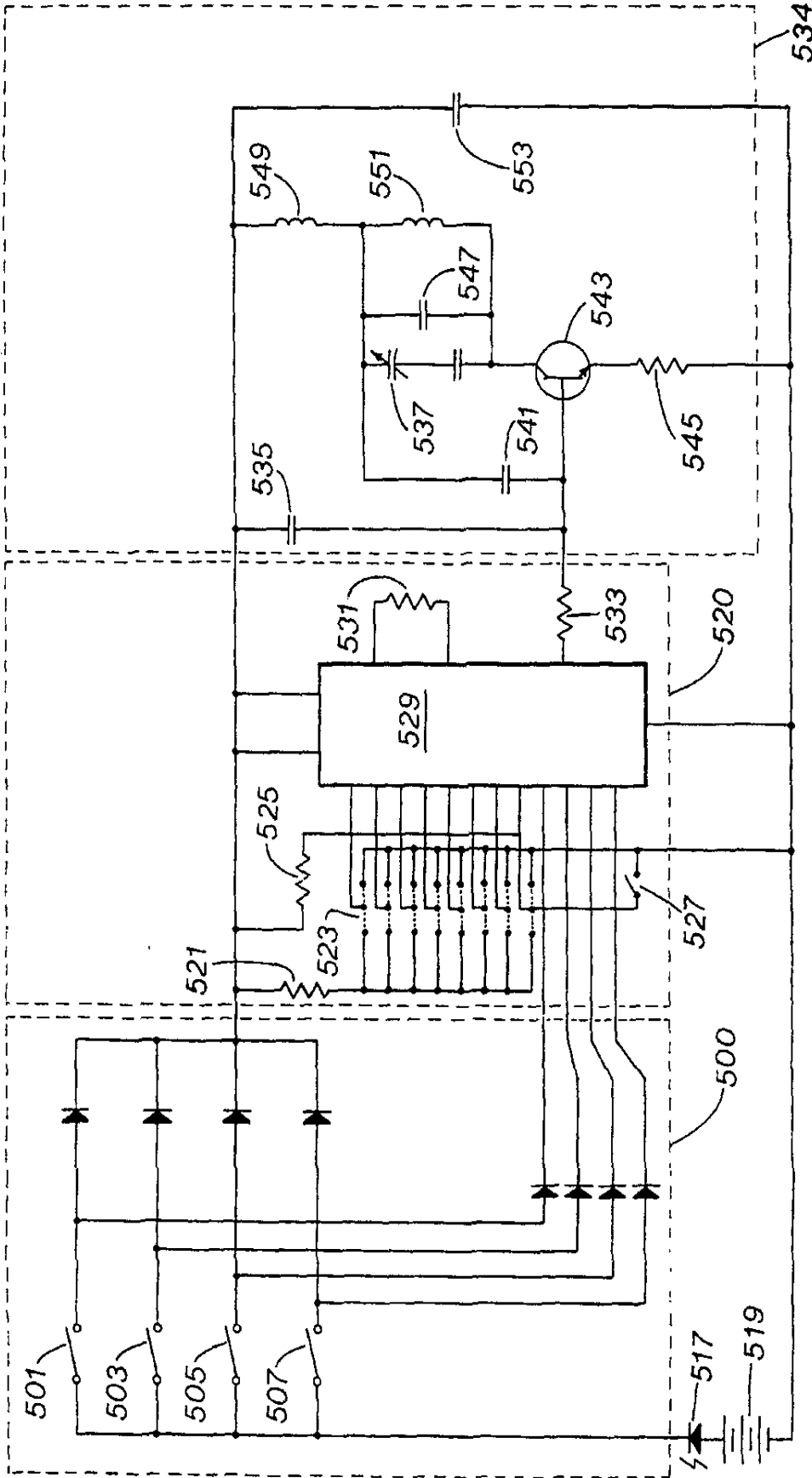


FIG. 4

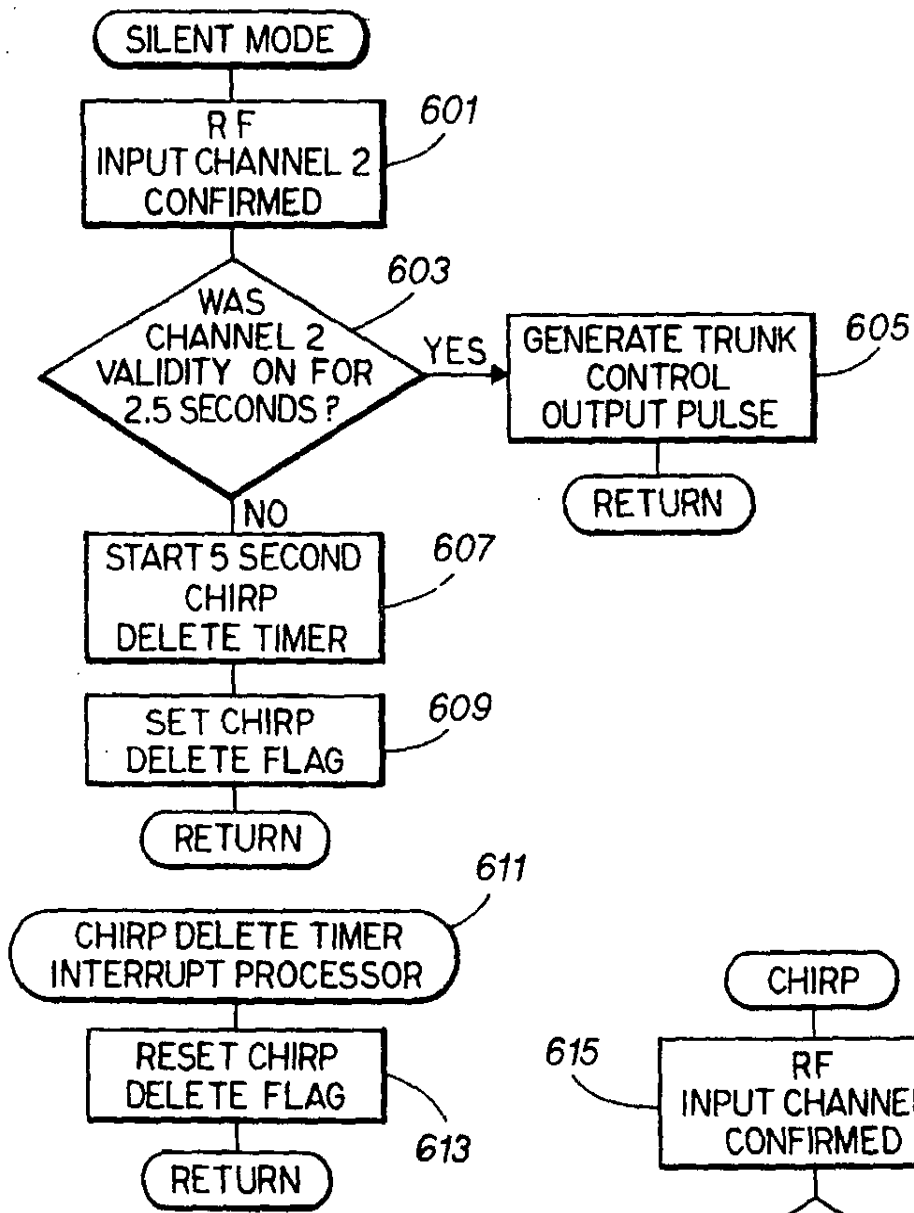


FIG. 5A

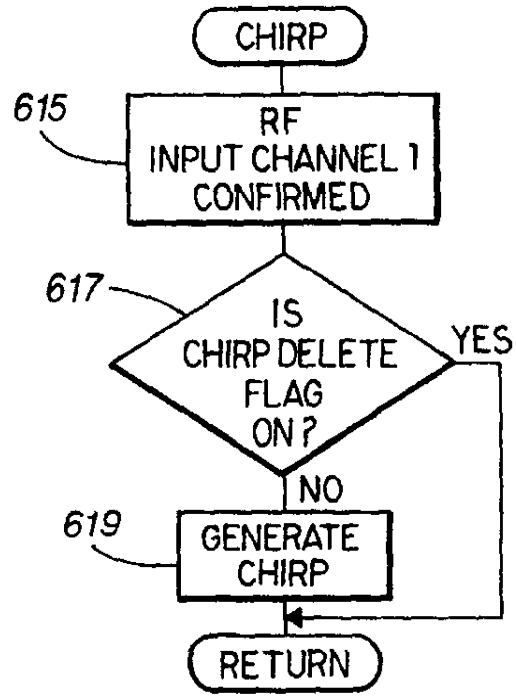


FIG. 5B

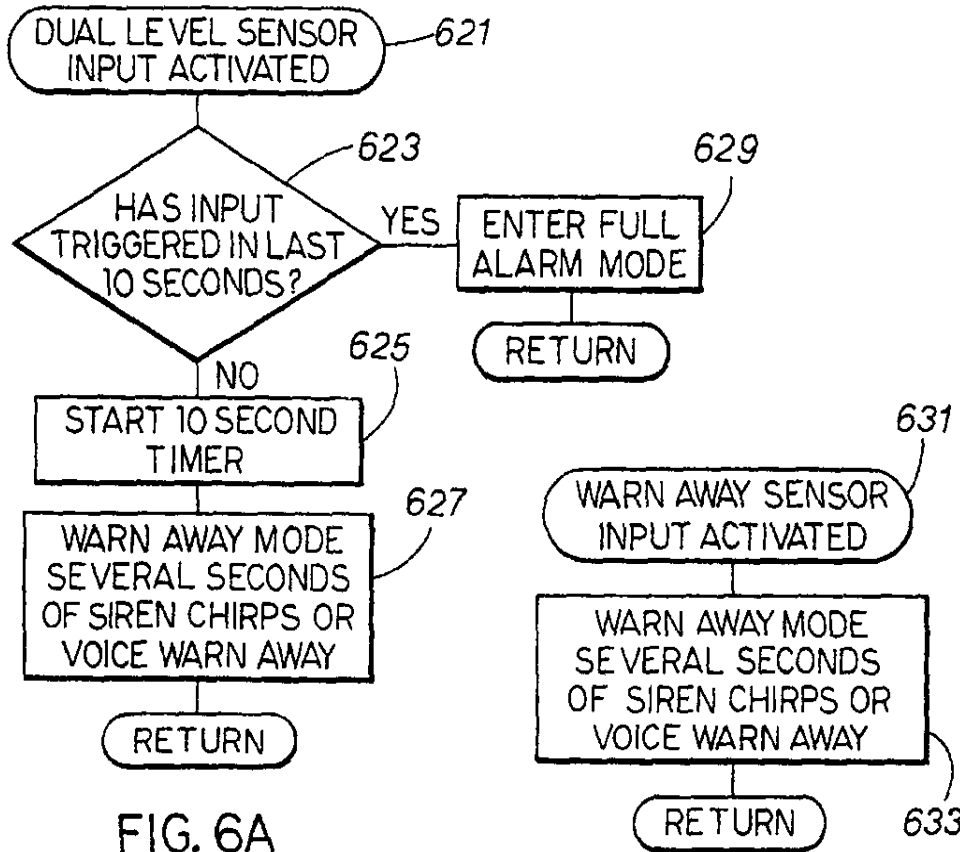


FIG. 6A

FIG. 6B

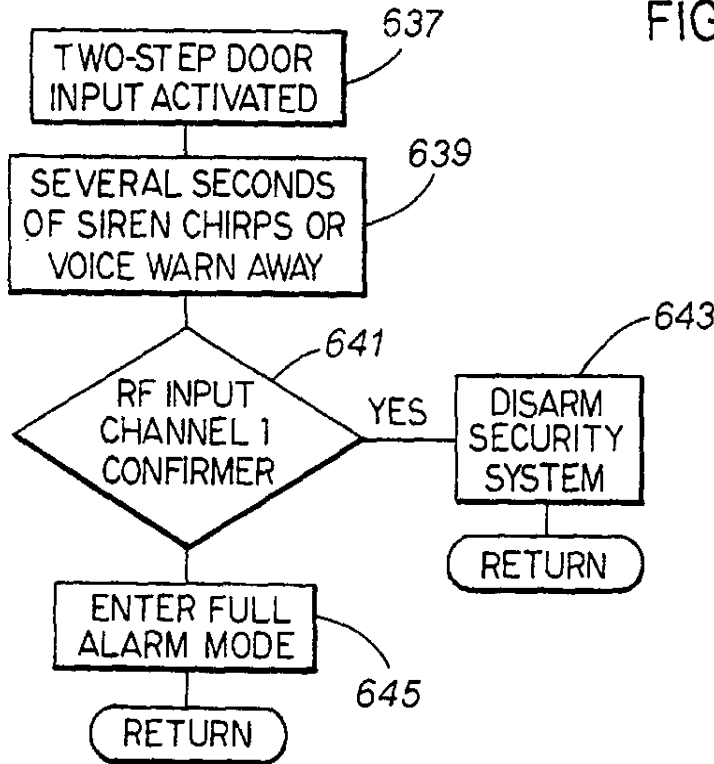


FIG. 6C

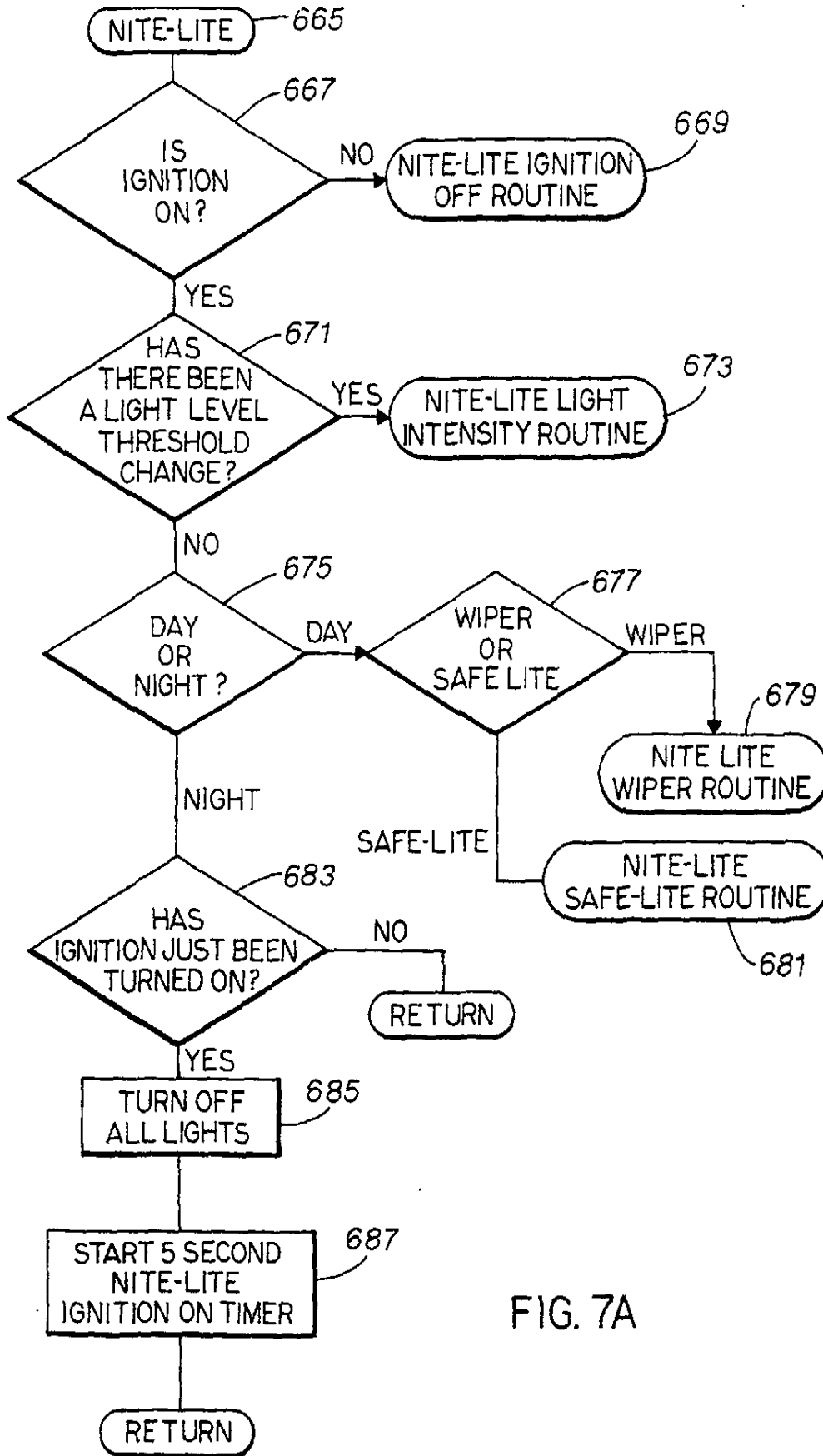
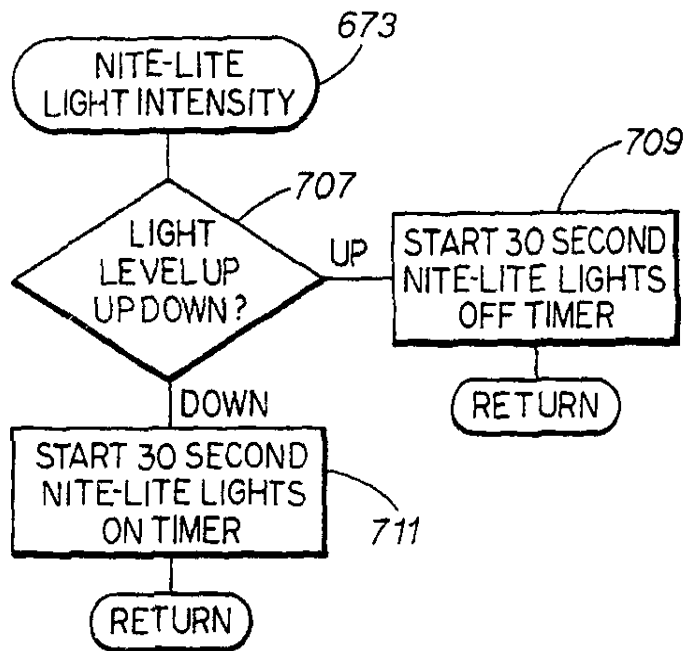
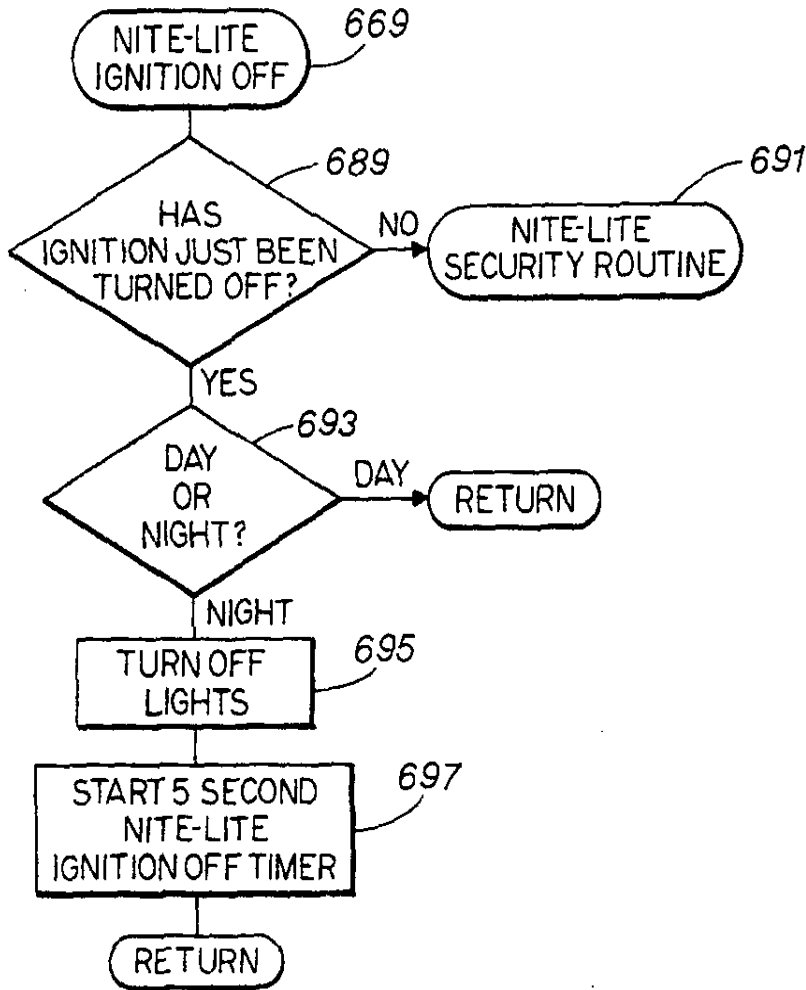


FIG. 7A



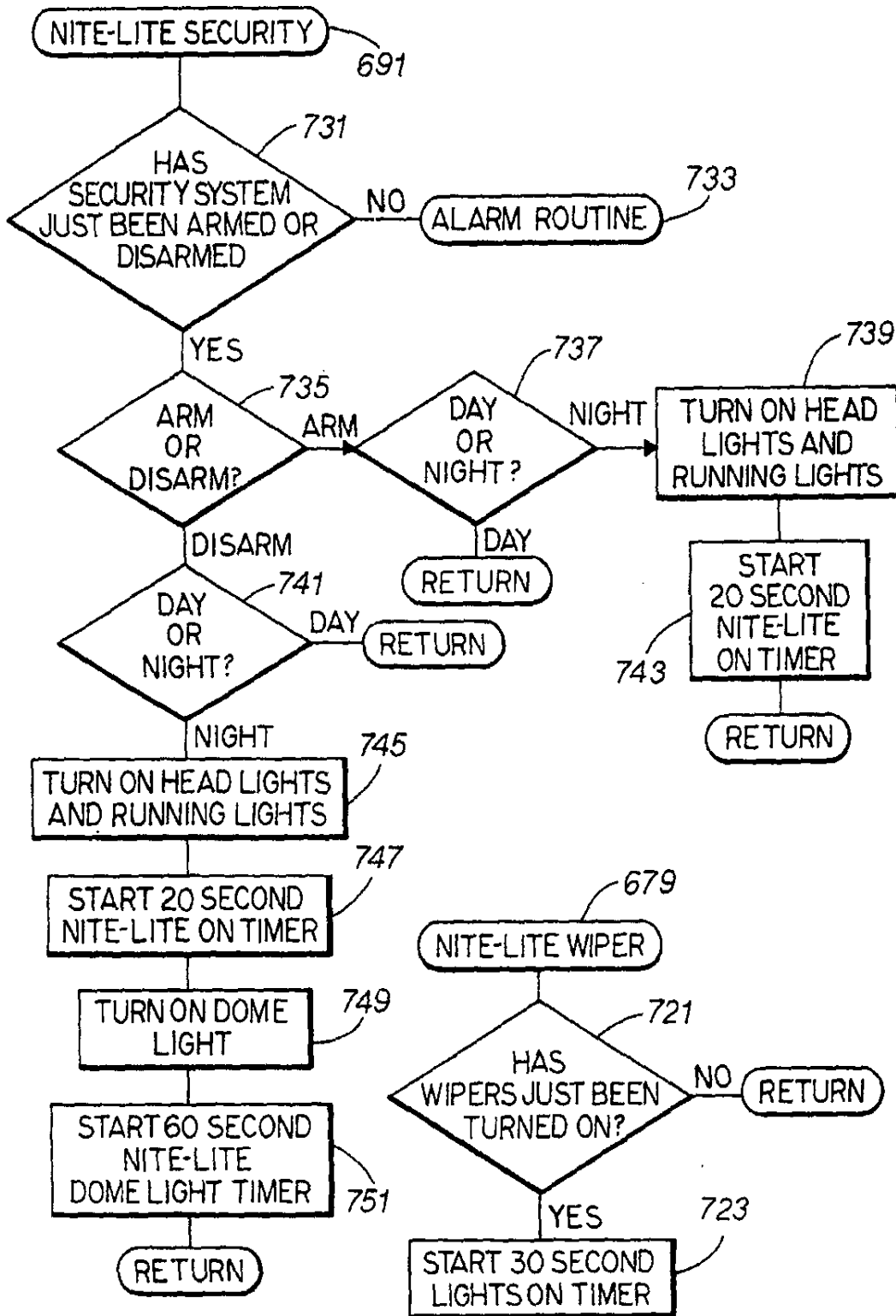
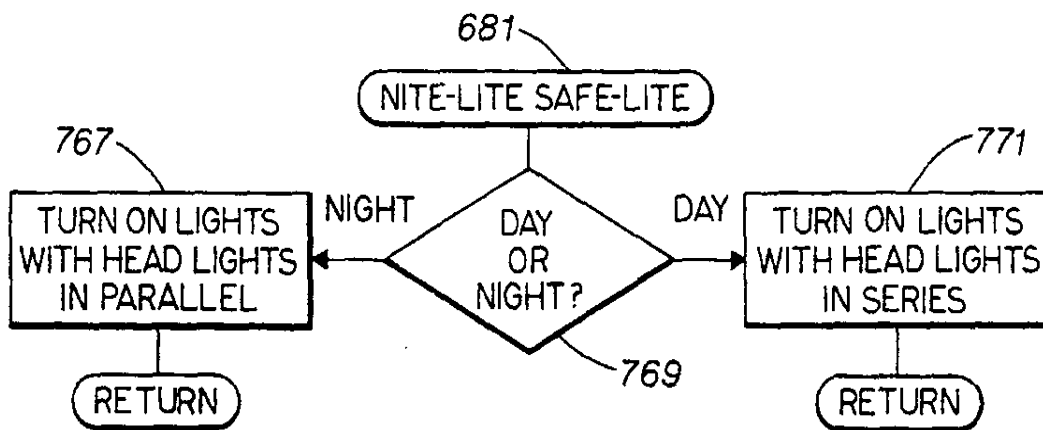
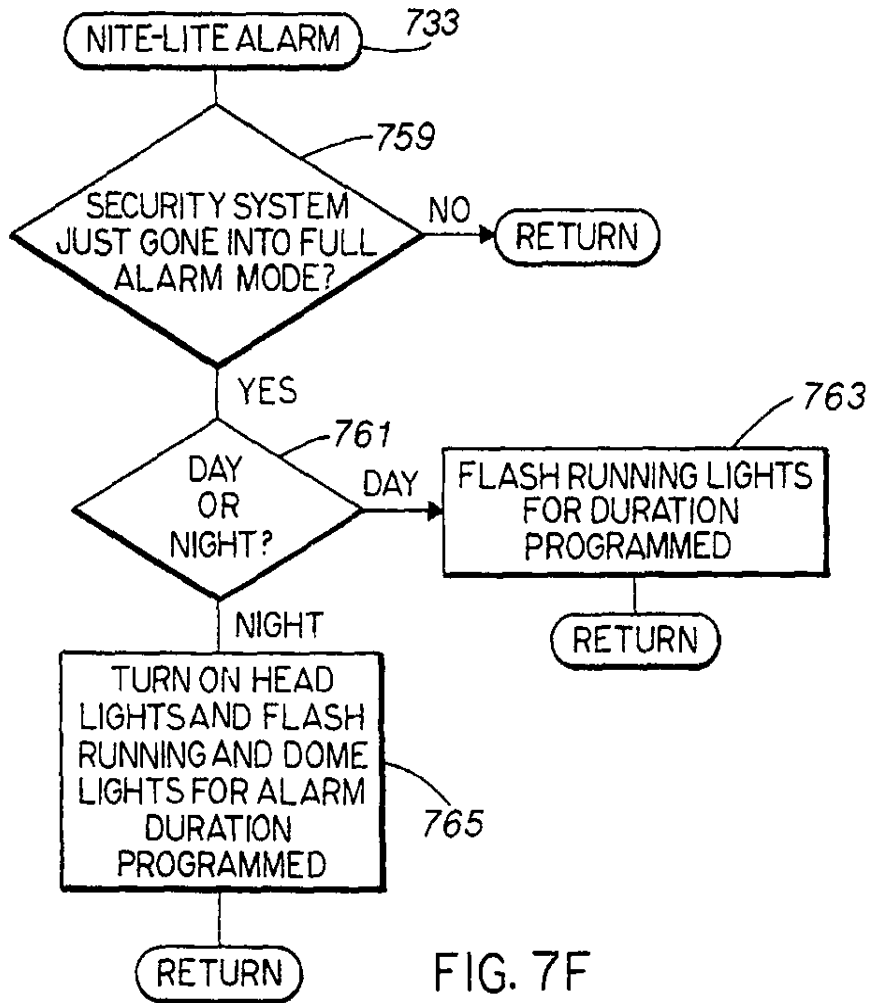


FIG. 7E

FIG. 7D



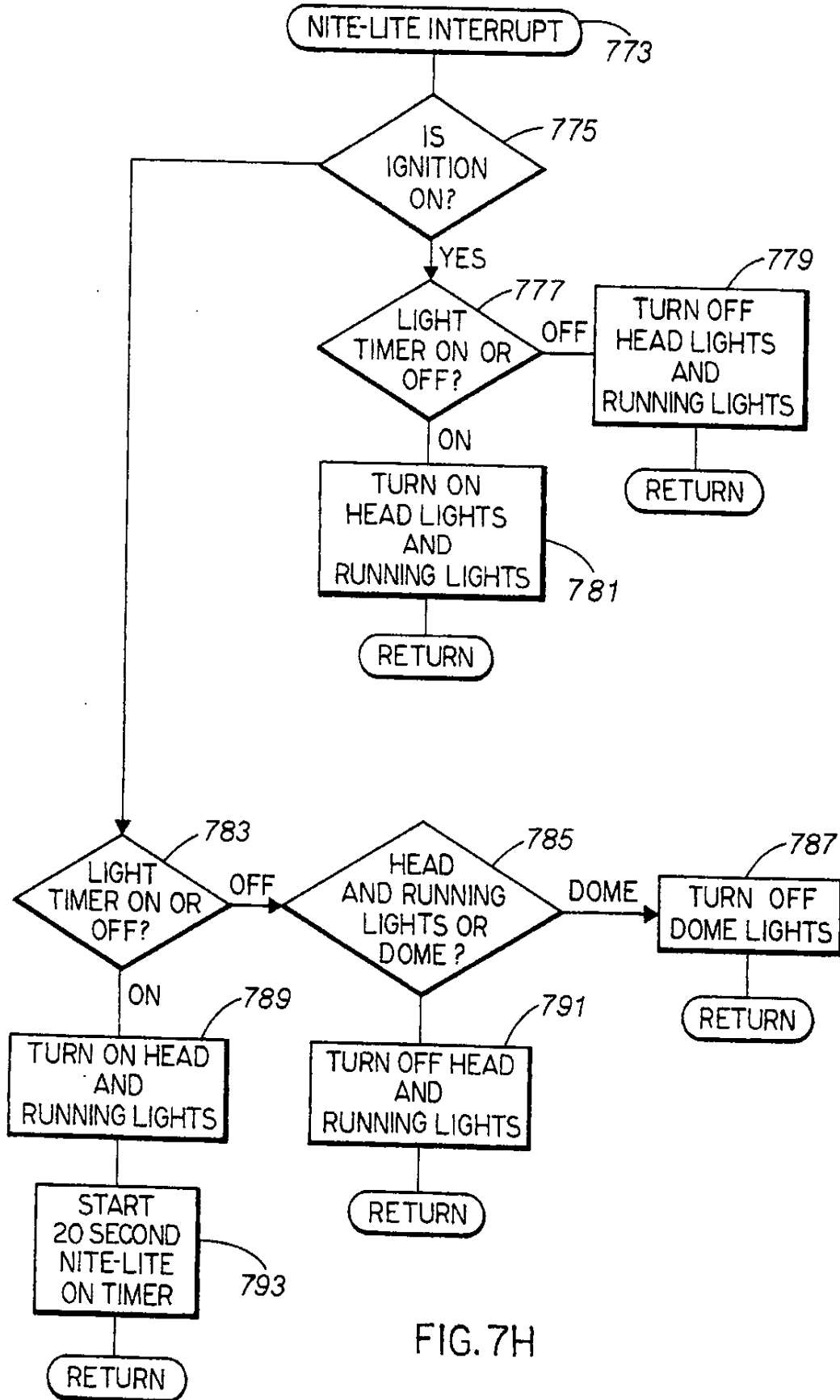


FIG. 7H

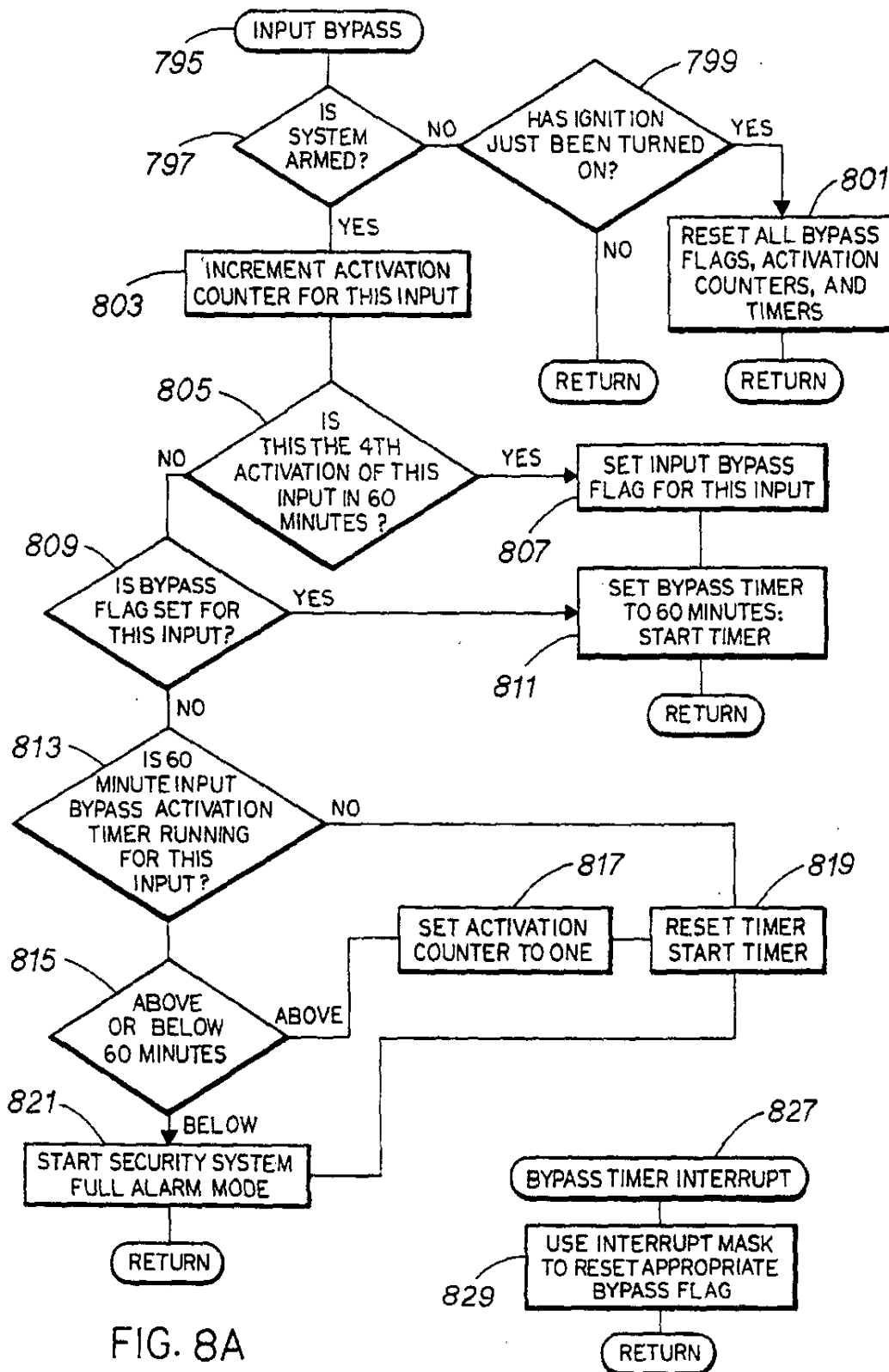


FIG. 8A

FIG. 8B

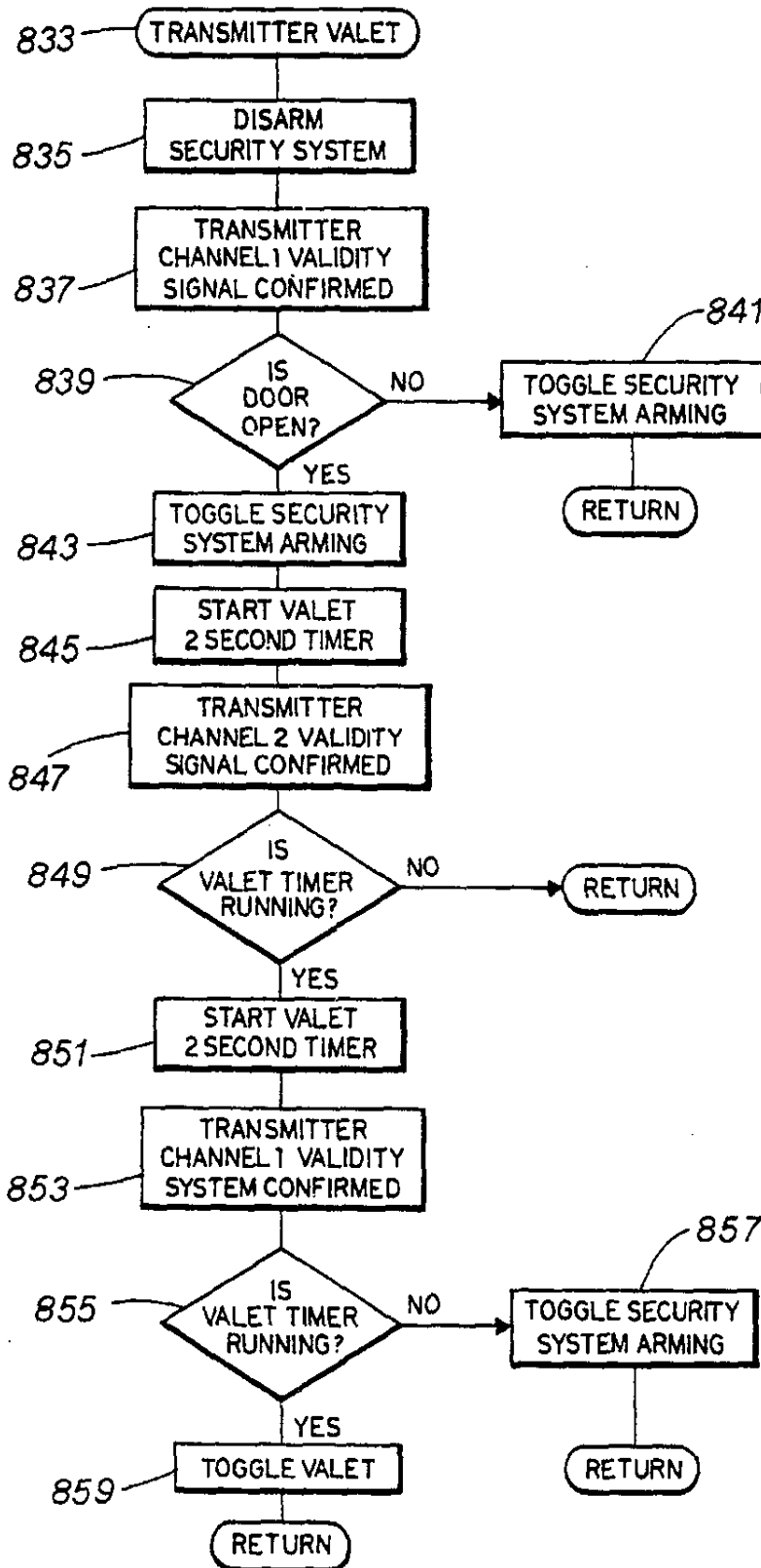


FIG. 9

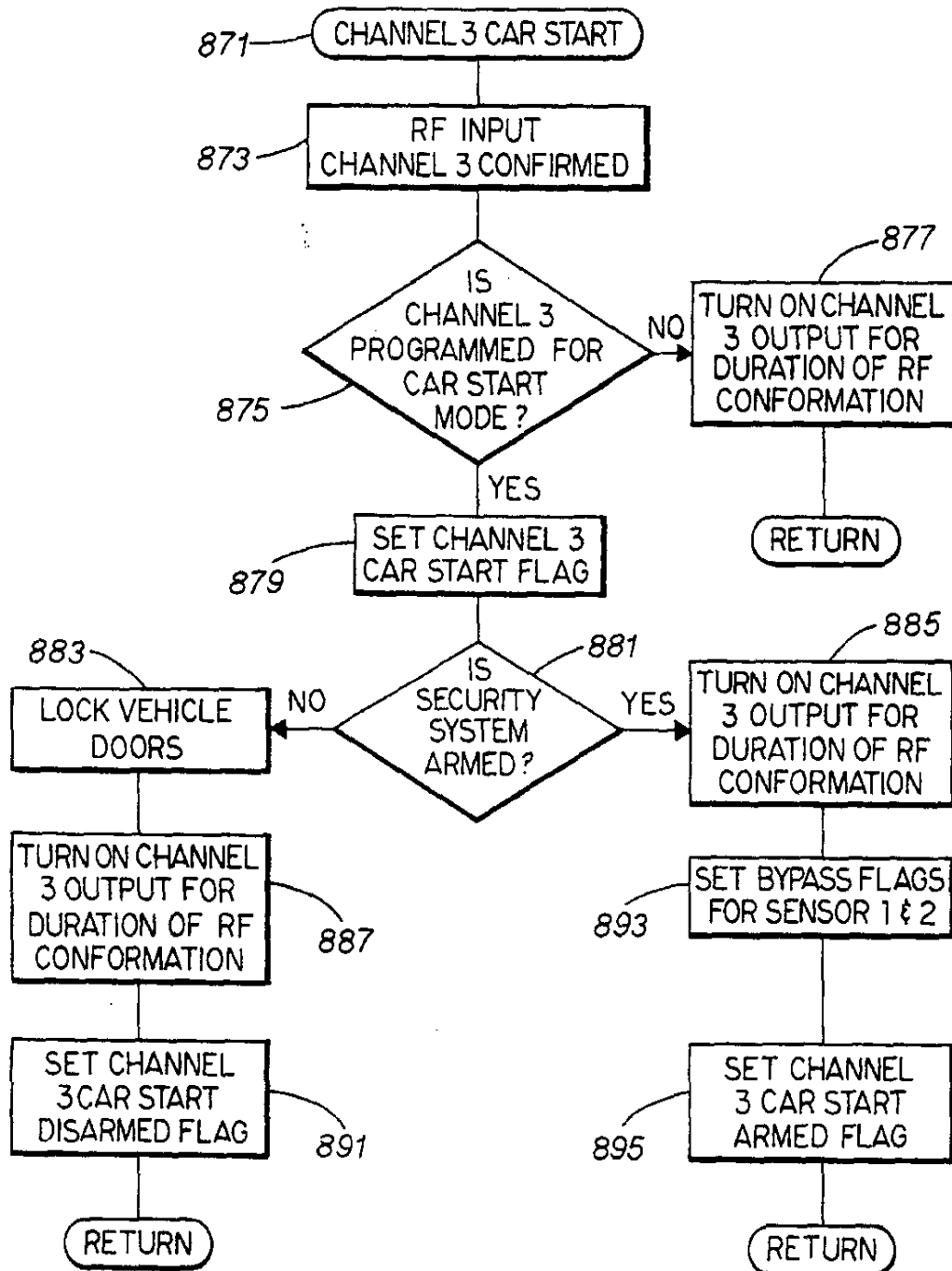
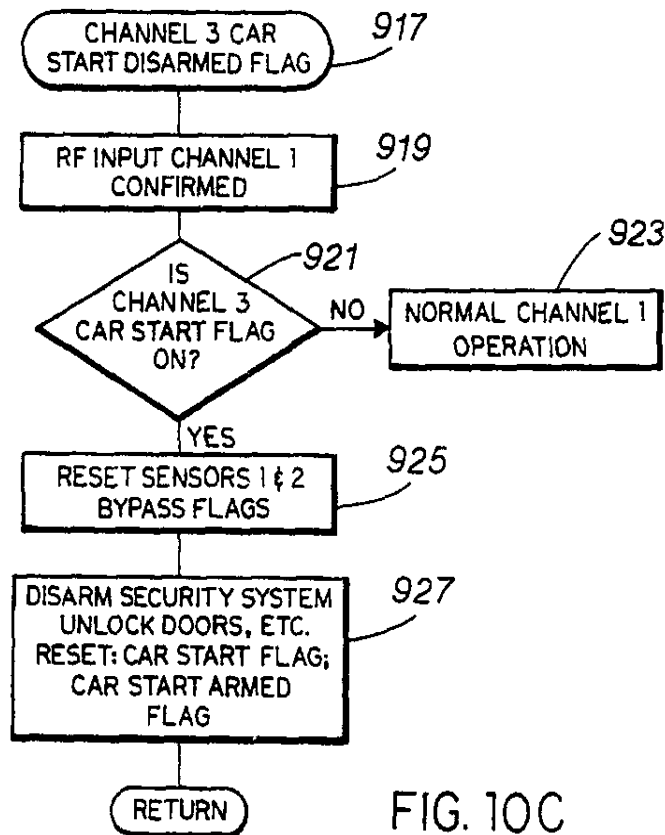
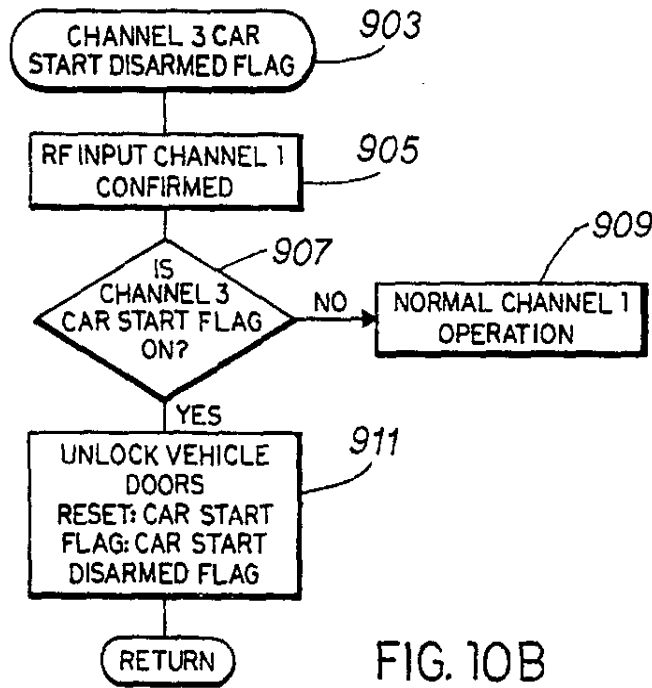
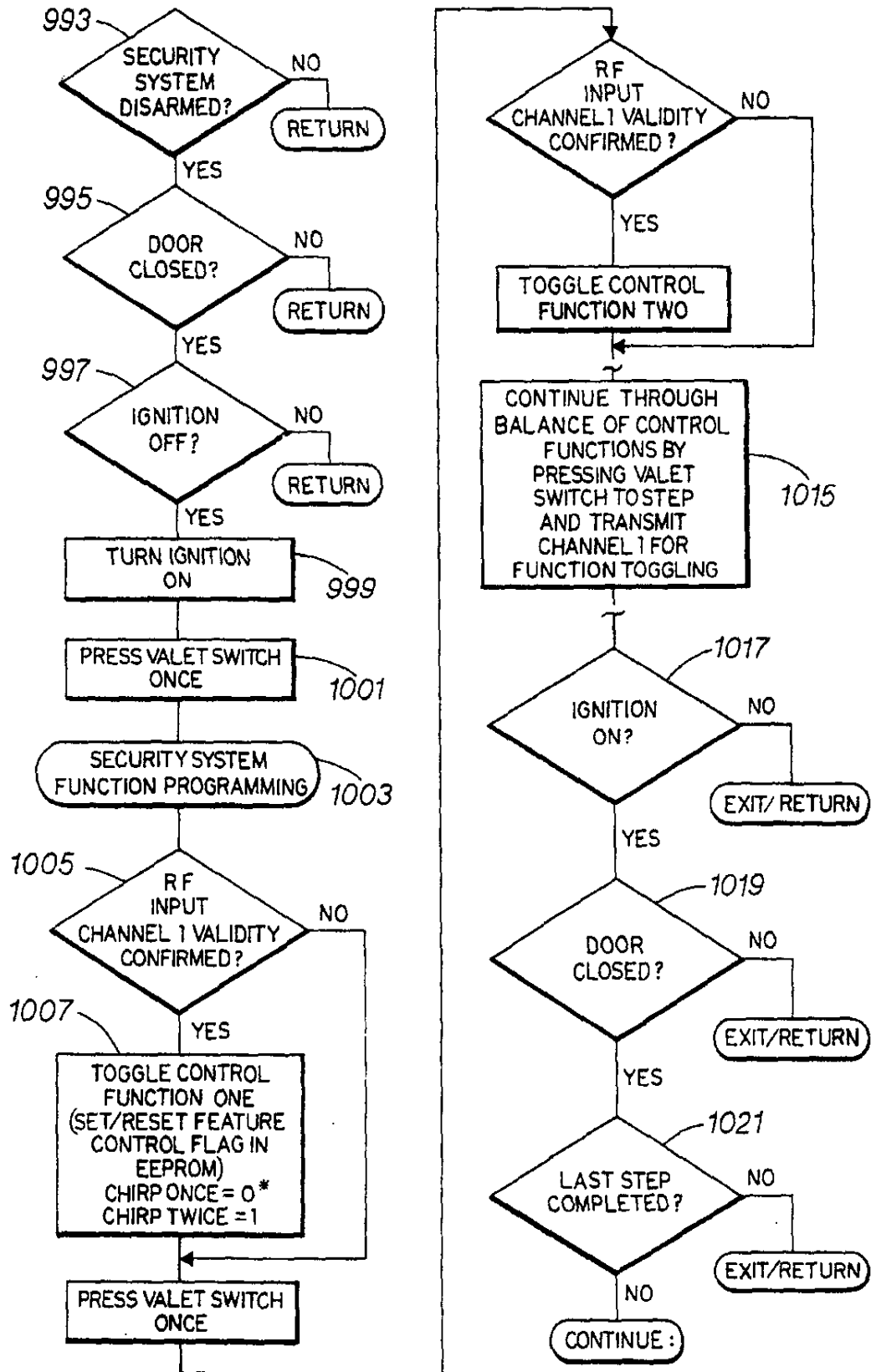


FIG.10A





* FACTORY SETTING

FIG. 11

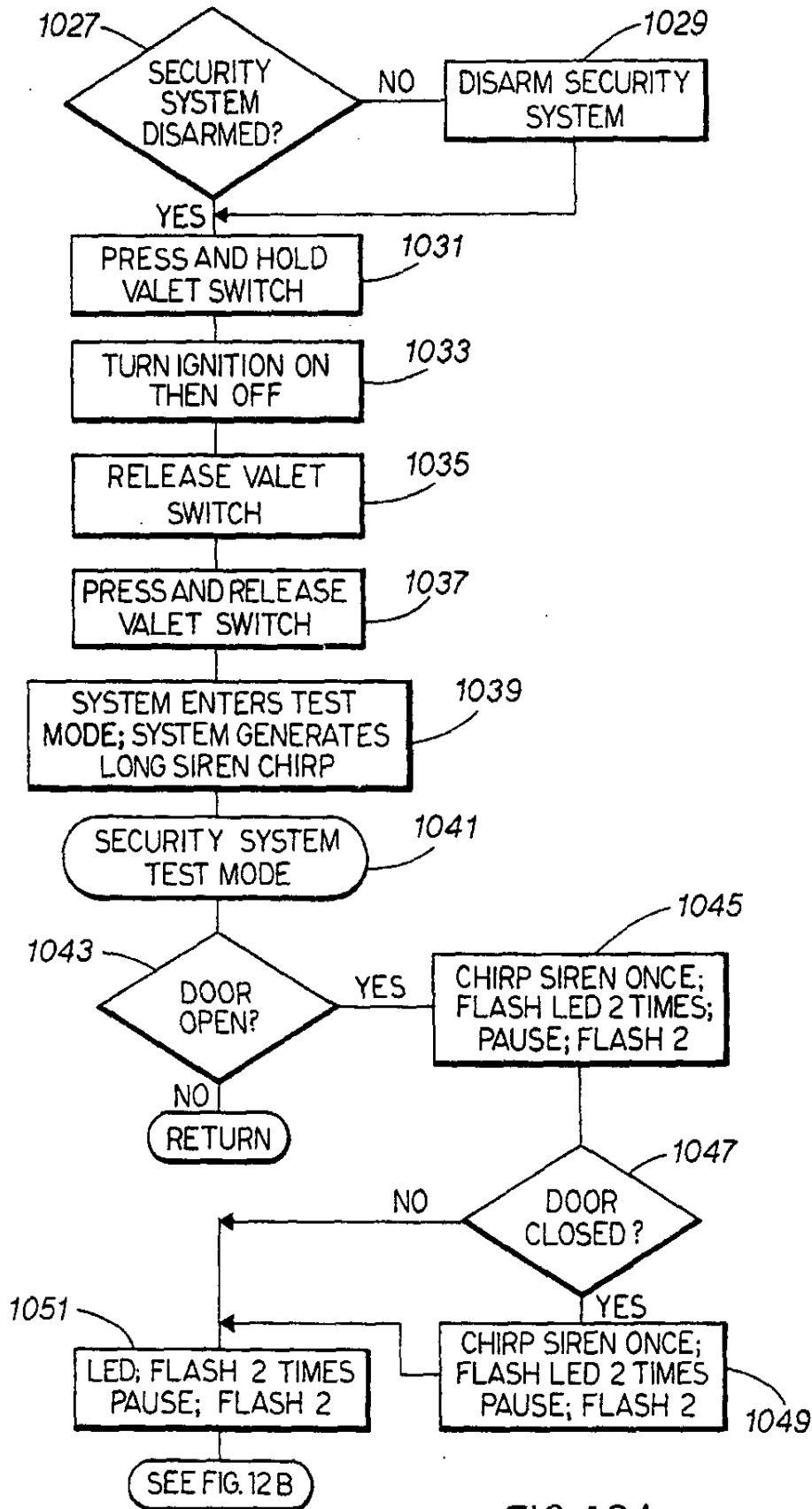


FIG. 12A

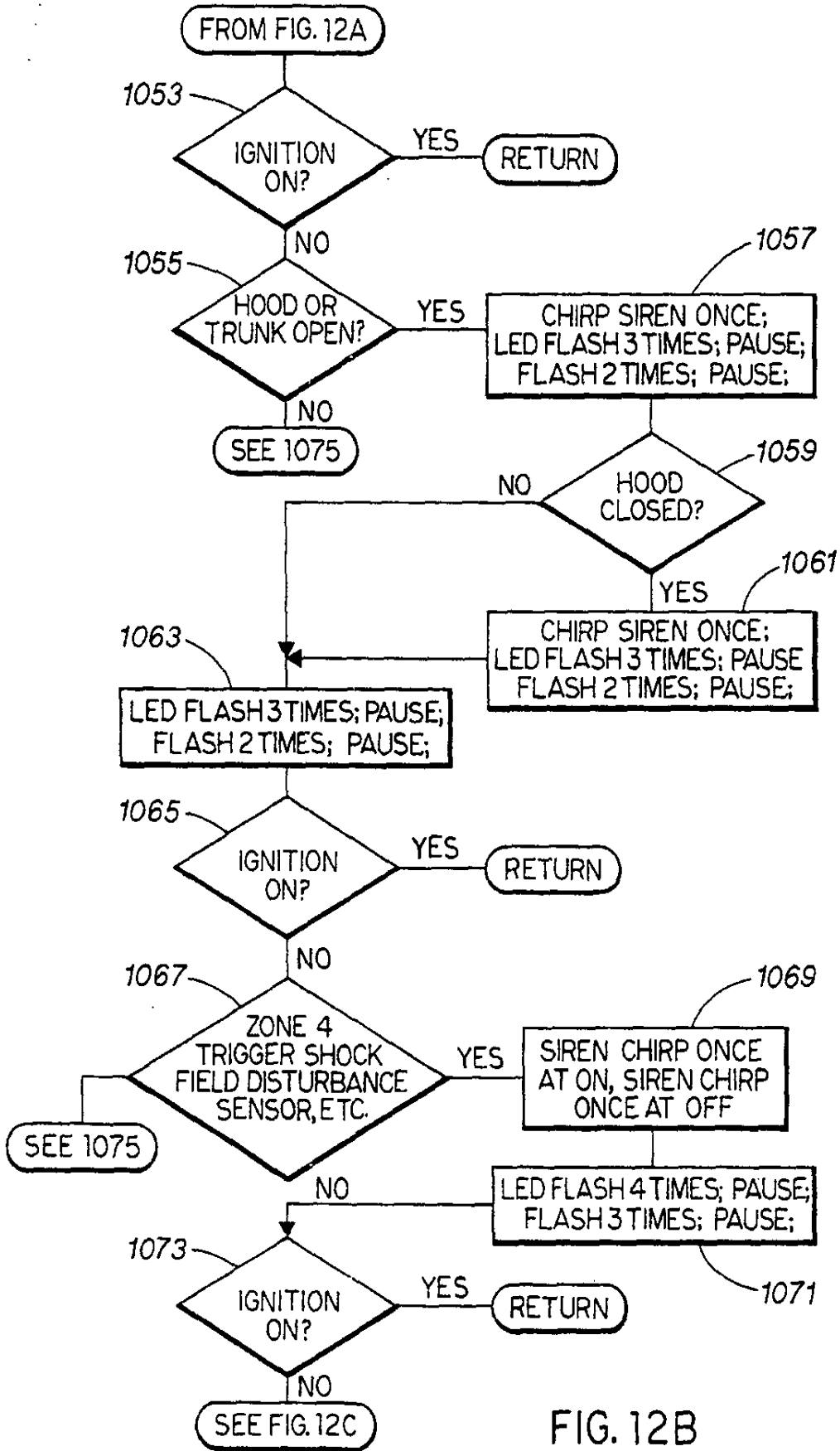


FIG. 12B

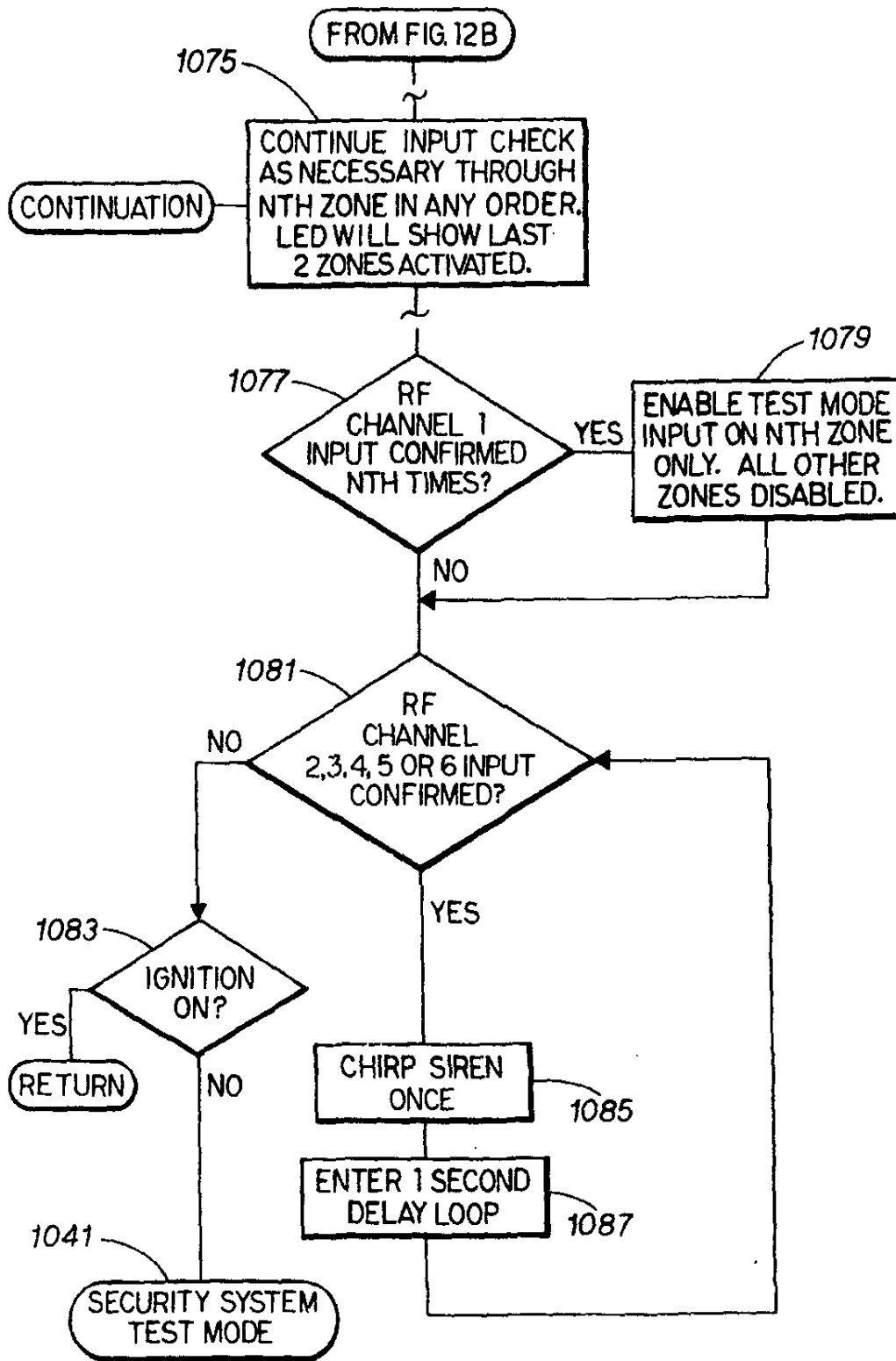


FIG. 12C

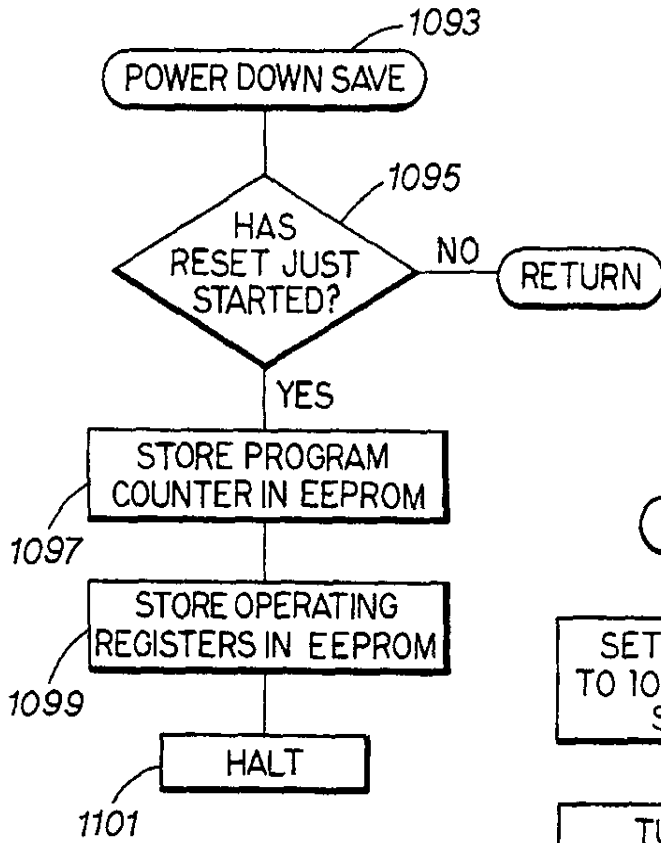


FIG. 13

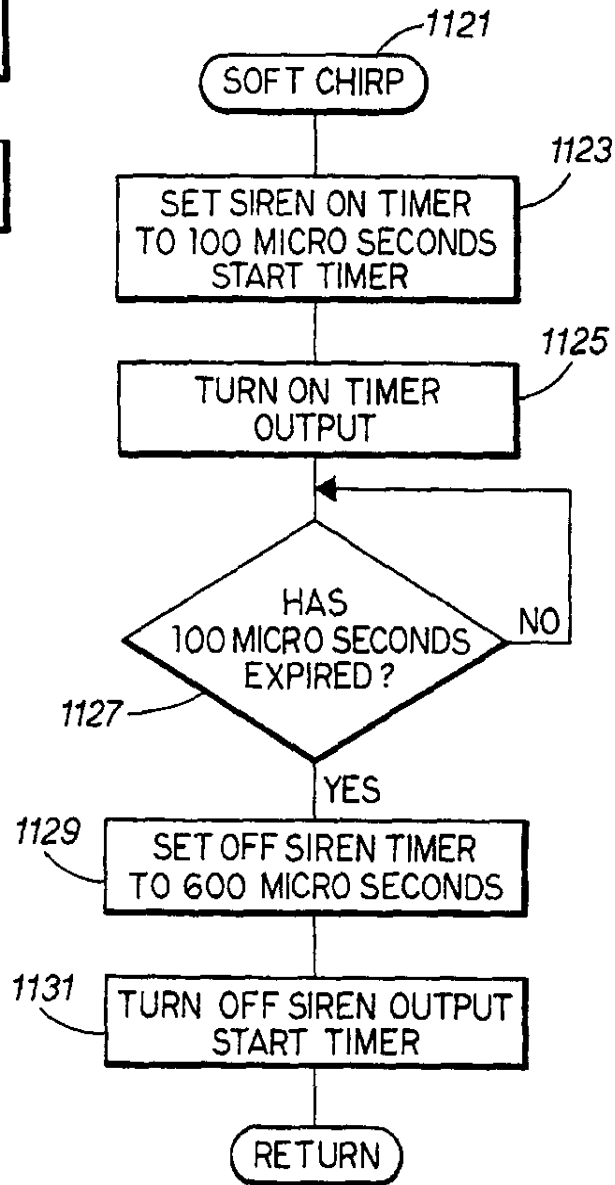


FIG. 14

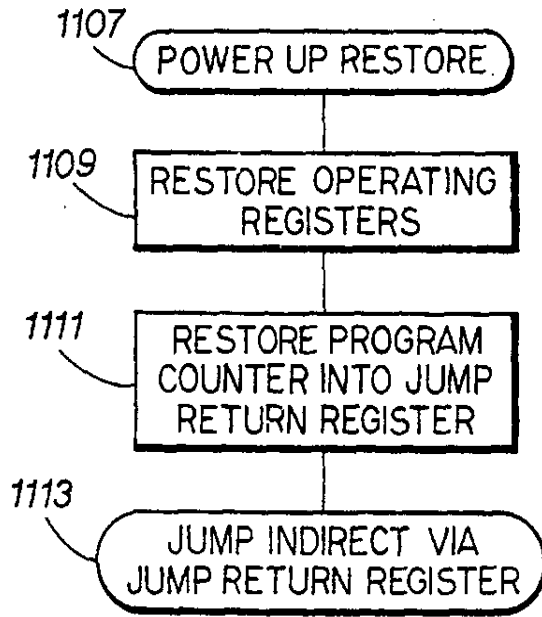


FIG. 15

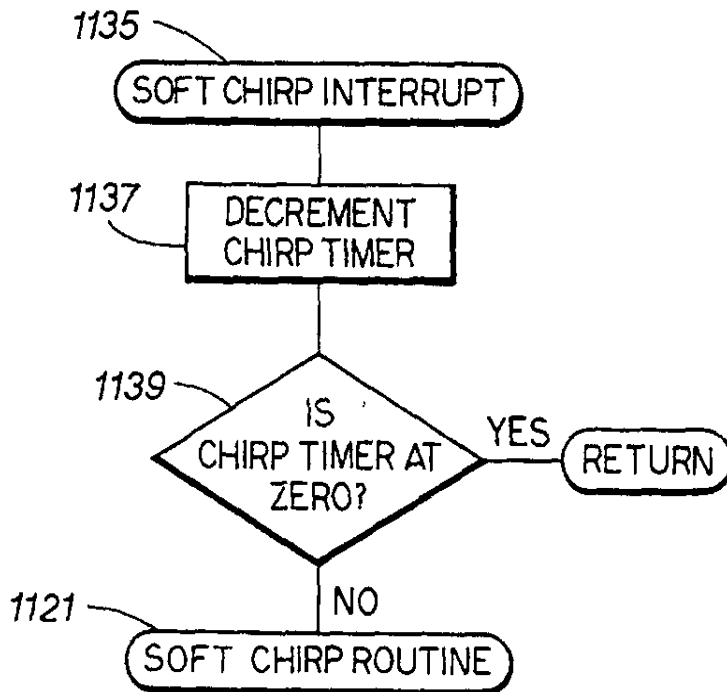


FIG. 16

5,534,845

1

ADVANCED AUTOMOTIVE AUTOMATION AND SECURITY SYSTEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to the field of security systems for monitoring restricted areas, such as in and around a vehicle. More particularly, it relates to a vehicle security system providing more features, greater range of operator-system interface, and more user-friendly operation than those systems in the prior art.

2. Description of the Prior Art

Electronic security systems have been in use for many years monitoring or controlling access to secured or restricted areas. These security systems normally use several sensors or trigger devices for monitoring an area of restriction. Normally a central controller monitors these devices and takes the appropriate action required by upon receipt of an input from one or more sensors. Examples of such security systems would include vehicle and home or business security systems. In today's art many of these security systems are controlled by a radio frequency pulse-width-modulated remote-control transmitter. The pulse-modulated radio frequency remote-control transmitter signal is digitally encoded to match the coding of the central controller's decoder, thereby restricting access of the security system to the allotted operators.

Security systems are no longer just security systems, but personal convenience systems as well. Vehicle security systems today offer the operator many new, advanced features that were not even considered a few years ago. Today the radio frequency remote-controlled vehicle security system provides remote door locking/unlocking, remote trunk release, remote window roll up/down, and remote vehicle starting, to mention a few of the newer features.

Most remote-controlled security systems today use both an audible and a visual arm/disarm notification signal to verify arming and disarming of the security system. On many occasions, this would be considered a nuisance because it could disturb people in an apartment complex, in a parking garage, or any residence when someone arrives in late at night. Most vehicle security systems today have some method of permanently disabling siren chirps (audible notification signals), but this does not give the user the flexibility of choosing when to generate audible notification signals. A few security systems accomplish this by a radio frequency remote-control transmitter, but those lose something in the process. One such system delays the chirps (remote RF signal confirmation) until a second input on the control channel is received or not received (the arm/disarm notification is just delayed). Another uses a second remote channel to disable the chirps, but loses use of that channel for other purposes.

As of today no known security system uses a light sensor to control the vehicle's light systems. There are light sensor products for vehicles on the market, but none are built into a security system. Some use a light sensor to turn on lights, others turn on lights when the wipers are turned on, and some use a light sensor in vehicle convenience systems.

Most security systems with input diagnostic and bypass capabilities allow as many as 10 full alarm trips, triggered by one input, before disabling that input. If an alarm cycle is reset by the security system's remote-control transmitter, the input is re-enabled; and there is no timer to re-enable the input if the input stabilizes or the environment changes. With

2

today's sensors and the high sensitivity to which the user wishes them to operate, it is not uncommon for a sensor to develop some periods of instability, particularly with changes in the environmental conditions. Most of today's security systems do not allow a sensor back into the system once it has been disabled until the security system is disarmed and rearmed.

In present-day security systems, a "hidden" switch may be manipulated by the owner to turn off the security system and allow the remote-control transmitter to be used only to lock and unlock the doors. This is called the "valet" mode and is used for vehicle servicing, etc. Valet mode is a set condition of the security system in which the operator may have control of convenience features, but all alarm functions and outputs are disabled.

One of the convenience features of today's remote security systems is the capability to add a remote car starter. This allows operators in extreme cold climate areas to remote-start their vehicles to prevent engine block freezing, and to start their vehicles in the morning to warm the vehicle. During hot periods, operators may pre-cool their vehicles before they get in to drive. Usually when a vehicle is started by remote control, the security system must be disabled in some manner, otherwise the vibrations, voltage surges, and movement of the vehicle, would activate the alarm.

The programming of operational functions on most of today's security systems is accomplished through switches, jumpers, and input/output selection. This means the user or installer, if required, must access the control module to change any of the operational functions of the security system. This is a nuisance in that most times the control module is buried under the dash, under a seat, or behind a kick panel. This limitation of the user interface with the system is a major problem with today's security systems.

The testing of one of today's complex security system's installation can be a long and tedious task. The installer must check all the inputs to make sure that they are properly connected. He or she must also check all of the outputs to verify that they operate properly. They also must check that the security system has proper range for the RF remote-control transmitter. One existing system has a built-in test mode which is referred to as a "real time zone monitoring diagnostic mode" and a "RF performance mode". However, in these cases the installer requires assistance on the inside of the vehicle to monitor the LED or speaker. Other security systems have to be continually armed and disarmed while these tests are conducted. This is a tedious task, but it also could be damaging to the security system or vehicle since each time a security system is armed or disarmed the doors are locked or unlocked, the lights flash, and the siren chirps.

As stated in previous patents, one way an intruder gains access to a secured area is to remove and restore power to the security system, which on many older security systems will leave the security system inactive. Most of today's security systems will restore to full alarm mode when power is reapplied, unless a certain condition is preset before power is restored.

The audible chirps or synthesized voice signals of today's security system are quite loud in a low-noise environment, which can be a nuisance under many situations. These audible signals are always of the same intensity day or night, in a busy parking lot, in a hospital zone, etc. Some security systems have the capability to completely silence these audible signals, but none have the capability to reduce the volume of these audible signals within the control module.

SUMMARY OF THE INVENTION

This invention is a automotive automation/vehicle security system that overcomes all of the problems described

5,534,845

3

above. It provides more features, greater range of operator-system interface and more user-friendly operation than those systems in the prior art.

The problem of the chirps creating a nuisance is overcome in the disclosed security system by a means for silencing the security system arm/disarm notification chirps from the system's remote-control transmitter. When the programmed channel 2 remote-control signal is confirmed, the controller starts a 5-second quiet period, during which, if a security system arm/disarm occurs, no audio notification signal output will be generated. Therefore the security system arm/disarm notification will be indicated entirely by the system's visual devices (running lights will flash and the status of the LED output will change).

The problem of a full alarm response being a nuisance is overcome by the security system providing multiple levels of sensor input, which in turn causes the controller to generate multiple levels of alarm output. With the lowest level of threat, the first level of sensor input will never cause the security system controller to generate a full audio and visual output. The maximum response to any activation of this input is several seconds of siren chirps or synthesized voice message. The second level of input will always respond to the first activation of the second level input within any short period, such as 10-seconds, with the same output as the lowest level of threat input above, but any subsequent input within the 10-second window initiated by the first (second level) input will cause the controller to generate a full alarm response. This feature of the invention fully utilizes the capability of many of today's dual-level sensors. The third level input (the door input) is a two step input in that the first several seconds of alarm are siren chirps or synthesized voice message, after which will always follow the full siren alarm mode, unless the security system is disarmed by the user. The fourth level of input is the normal alarm instant input, which initiates a full alarm mode immediately upon being activated.

The security system of the invention introduces a new feature that increases the convenience of automotive automation/security systems. It uses a light-sensor input to allow the security system controller to control the vehicle's light systems. The Nite-Lite feature uses the light sensor to measure the level of light to control the light systems of the vehicle under various circumstances. The security system also controls the lights under other circumstances associated or not associated with light sensor.

In daytime, the only lights that are turned on are the running lights, which are flashed during the full alarm mode and when the security system is armed or disarmed; with the exception that when the windshield wipers are turned on, they override the light-sensor control and turn on the headlights and the running lights for driving during rainy conditions. At night or under low light conditions, the headlights, running lights, and dome lights could be turned on; depending on the mode of operation. While driving, the headlights and running lights turn on automatically when the light level drops below the light-sensor lights-on-threshold, and off when the light level goes above the lights-off-threshold. When the security system is armed, the headlights and running lights turn on for 20 seconds. Upon disarm, the headlights and running lights turn on for 20 seconds, and the dome lights turn on for 60 seconds or until the ignition is turned on. During a full alarm mode, the headlights turn on and the running and dome lights flash. When the ignition is turned off, the lights go out for 5 seconds if on, then the headlights and running lights turn on for 20 seconds. If any lights are on when the ignition is turned on, they will turn

4

off; five seconds later, the headlights and running lights will turn on for driving.

The problem with temporarily disabled sensors and the prior-art approach to remove them from the security loop is solved in this invention by the addition of circuitry that re-analyzes the unstable sensor at a later time and then, if the sensor is found to be stable, the sensor is returned to the system. If any prolonged sensor instability is detected, that sensor is bypassed for a stable period of one hour. If the sensor input in question activates the full alarm mode three times in one hour, that input is bypassed upon the next activation without entry into the full alarm mode. If the input stabilizes for a period of one hour, it is re-enabled. If the bypassed input is activated inside that one-hour window, the one-hour timer is reset to one hour and restarted. The only way the bypass flag can be reset is for the timer to expire or for the ignition to be turned on while the security system is disarmed. Even if the security system is reset while in the full alarm mode via the system's remote-control transmitter, the bypass counter would be incremented and if the count was then four, the bypass flag for this input would be set, bypassing the input in question.

Another problem solving feature of the invention includes means for placing the security system in "valet" mode or removing it from "valet" mode using the remote-control transmitter and one of the vehicle's doors. This is accomplished by opening a door of the secured vehicle and transmitting remote control signals from channel 1, then channel 2 within two seconds, and again channel 1 within two seconds. This toggles the valet mode; if valet is on, it is turned off, or if valet is off, it is turned on.

The problem of losing security and safety while remote starting a secured vehicle is solved by this invention. This invention allows the user to remote start the vehicle while at the same time continues to provide full security to the doors, trunk, hood and windows. Thus remote starting may be provided with real security and safety being continued on the vehicle. If the security system is armed when the remote-control transmitter car-start signal is initiated, the security system will bypass some of the sensors before issuing the car start output signal. If the security system is disarmed when the remote-control transmitter car-start signal is initiated, the security system will lock the vehicle's doors before generating the car-start output signal, giving the user more security and safety. This feature requires a remote car-start control module for implementation of the remote car-starting and may be user-programmed to maintain security and safety when the car start output is generated.

An additional problem solving feature of the invention is the means for using the remote-control transmitter and valet switch located within the cabin to program, system. Once entered into the function programming mode, the user may depress the valet switch to select the function to be programmed, then toggle that function by using the remote-control transmitter. The security system will generate siren chirps, to indicate the mode of the system operational function: one chirp to signify factory default and two chirps to signify an alternate mode. By depressing the valet switch, mounted on the dash, and transmitting with the remote-control transmitter, all system-programmable operational functions may be selected and programmed. This overcomes the need to access the control module to change system operational function programming, which in most cases with today's security systems would require the user return the vehicle to the dealer/installer.

The installer benefits most from the next feature of this invention because he or she will not require any assistance

5,534,845

5

in testing the installation. The user also benefits in that the installation may be tested quickly and efficiently reducing the cost of the installation. Means are provided for the security system to be tested using a highly advanced installation test mode. The security system-test mode is entered by generating certain inputs in a predetermined sequence. For instance, the user or installer may undertake a simple program, such as disarm the security system, press and hold the dash mounted valet switch, turn on the ignition, turn off the ignition, release the valet switch, then press and release the valet switch once more enter the "test" mode. The disclosed security system will respond with one long chirp to indicate it has entered the test mode. While in the test mode, the user may test any of the operational inputs. The security system will respond with a siren chirp when the input goes active, and another siren chirp when the input goes inactive. At the same time, the security system's light-emitting-diode will indicate the last two inputs activated. By using the remote-control transmitter's channel 1, the user may select one input to test, which will disable all the other inputs. The user can step through all the inputs in this mode by pressing the remote-control transmitter as many times as the zone of the input to be tested. One of the most important features of the security system test mode is the remote-control transmitter range test.

System radio frequency remote-control transmitter range is a major problem with some installations due to interference from inside the vehicle or the placement of the control module, which contains the RF receiver. The RF range test is accomplished by transmitting a control signal on any remote channel other than channel 1. As long as one of these auxiliary remote-control transmitter inputs is active, the security system will respond by generating a siren chirp once a second. This allows the user to test the range of the system by walking away from and around the vehicle while pressing one of the remote-control transmitter buttons.

A problem solving feature of this invention is the restoration of the security system's operational mode after a power failure. At power-down, all pertinent data is stored in permanent memory. At power-up, this data is restored to the system's random access memory and registers before the system's program is restarted. This feature allows the security system to be restored to the exact same conditions that existed at power-down. If the security system was in the armed mode at power-down, it will return to the armed mode when power is restored.

A nuisance reducing feature of this invention is to lower the output volume of the siren chirps by varying the duty cycle of the siren power supply during the chirps. This invention also includes two means by which the security system can reduce the output voltage/power at the siren output to generate lower volume chirps. The volume of the output chirps may be fixed in the security system at a certain power duty cycle, controlled by security system program switches, or remotely controlled/selected with the system remote-control transmitter. In this way, the invention is extremely useful in and around hospitals and in other areas requiring the arm/disarm messages to be issued quietly. The user has the ability to change the decibel level of the audible arm/disarm notification outputs as well as to turn them off, using the hand-held remote-control transmitter.

Accordingly, the main object of this invention is a vehicle security system that provides the user with a better interface to the system, allowing him or her to select of a wide variety of unique features not easily accessible in existing security systems. Other objects of the invention include a vehicle security system that allows the user to turn off the audible

6

arm/disarm notifications by using the hand-held remote-control transmitter; a security system with several levels of sensor inputs that cause the controller to generate several levels of alarm output; a security system with a light sensor input and other inputs to control the vehicle light systems; a security system that provides means for re-analyzing an unstable sensor to determine if its stability has returned and return it to the security system if it has; a security system where the user may enter and exit the valet mode using the remote-control transmitter and one of the vehicle doors; a security system that provides a remote start output while maintaining maximum security and safety; a security system that allows the user to program system operational functions using the remote-control transmitter and the valet switch; a security system that allows the installer or user to test the system's operational inputs and the system's RF remote-control transmitter range with minimal effort; a security system that restores security to pre-power fail conditions when power is restored; and a security system that has the means for generating variable volume arm/disarm notification chirps.

These and other objects of the invention may be found from a close reading of the Description of the Preferred Embodiment taken along with the drawings appended hereto. The scope of protection sought by the inventors may be gleaned from a fair reading of the claims that conclude this Specification.

DESCRIPTION OF THE DRAWINGS

FIG. 1 is a simplified block diagram of a automotive automation/security system comprising this invention;

FIGS. 2A and 2B are schematic diagram of the control module of the security system depicted in FIG. 1, less the radio-frequency receiver;

FIGS. 2C and 2D are schematic diagrams of two alternate embodiments of the soft-chirp output feature;

FIG. 3 is a schematic diagram of the radio-frequency receiver section of the control module depicted in FIG. 1;

FIG. 4 is a schematic of the radio frequency remote-control transmitter depicted in FIG. 1;

FIGS. 5A and 5B are flow charts of the means for deleting chirps/soft chirps using the remote-control transmitter without losing any of the security systems other functions;

FIGS. 6A, 6B and 6C are flow charts of the feature allowing multiple levels sensor inputs controlling multiple levels of output device notification;

FIGS. 7A-7H are flow charts of the means for using a light sensor input to a security system, allowing the system controller to control the vehicle's light systems;

FIGS. 8A and 8B are flow charts of the means for monitoring the input sensors of the security system, to bypass them after a prolonged period of instability and, after a given period of stability or when the ignition is turned on, while the security system is disarmed, readmit them to the system;

FIG. 9 is a flow chart of the means for entering or exiting "valet" mode using the security system's remote-control transmitter;

FIGS. 10A-10C are flow charts of the means for remote-starting the vehicle while maintaining maximum security and safety;

FIG. 11 is a flow chart of the means for programing the selectable operational functions using the remote-control transmitter;

5,534,845

7

FIGS. 12A, 12B and 12C are flow chart of the means for testing a security system installation and its radio-frequency remote-control transmitter range;

FIGS. 13 and 15 are flow charts of the means for restoring a security system status after a power disconnect; and,

FIGS. 14 and 16 are flow charts of the means for generating soft chirps by pulsing the siren output during chirps or reducing the siren output voltage/current during chirping.

DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. 1 represents a simplified block diagram of the primary functional components of the automotive automation/security system of this invention. This invention may be used in other areas and the description of its use in a vehicle should not be taken as limiting it in any way. The security system generally involves the interaction between a user and the system controller to obtain the various functions and features of the invention. This invention includes a radio-frequency (RF) remote-control transmitter 25 and a control module 29. Control module 29 includes a RF receiver 33, which receives a digital encoded signal transmitted via receiving antenna 31 from remote-control transmitter 25 via its antenna 27. Controller 35 and an external electrically programmable and erasable read-only memory EEPROM 37. The incoming digital signal code is either presented directly to controller 35, for decoding, or as an alternate means to a system integrated circuit decoder for decoding to give the proper channel output corresponding to the transmitted channel.

The user may employ a plurality of system hardware to generate inputs, generally shown along the left side of controller 35, for communicating commands to the controller. Such hardware may include program switches, jumpers, or jumper pins, valet switches, ignition switches, and door switches. Most commands are communicated to the controller during normal use of the vehicle, such as turning the ignition on or off and opening or closing the vehicle door. The remote-control transmitter 25, in the hands of the operator or user, can issue operations, operational function programming, and operational testing commands to controller 35. These commands include a stream of 29 binary bits of data that are assembled in a fixed sequence to form the particular user code for a given command. These codes are preset by programming either by the manufacturer, the installer or the user.

The vehicle battery supplies power to the control module 29. The vehicle provides a nominal 12.6 volts direct current (DC) power to all powered inputs to the control module. Power supply 39 filters and regulates the power to supply either 5 or 12 volts as required to components of the control module. The RF receiver 33 power is further isolated and filtered by an additional resistor and capacitor (RC) filter 41. The remote-control transmitter 25 is powered by either a 9-volt or 12-volt miniature alkaline battery.

Remote-control transmitter 25 as shown in FIGS. 1 and 4, in the most preferred form, provides a pulse-width-modulated radio frequency signal, wherein an RF carrier at some predetermined frequency is modulated (turned on and off by variable pulse widths) by pulses from an internal encoder-integrated circuit 529. Remote-control transmitter 25 is comprised of the channel selection section 500, the transmit indicating LED 517, the battery 519, the encoding section 520, and the RF transmitting section 534. As is well-known

8

in the art, remote-control transmitter 25 is normally actuated by depressing one or more switches 501, 503, 505, or 507, located in the remote-control transmitter 25 casing, to generate a distinct RF signal encoded with the information from encoder integrated circuit 529.

Encoder 529 generates a 29-bit binary digital code; the pulse width of each pulse determines if the code bit is a zero or a one. The specific code of a particular remote-control transmitter 25 is determined by 12 trinary inputs controlled by cutting traces 523 and the remote-control transmitters switches 501-7. An optional resistor 525 and switch 527 allow the user to double the output channel capability of remote-control transmitter 25. LED 517 indicates when the remote-control transmitter 25 is active. Battery 519 supplies power through LED 517, channel selection section 500, to encoding section 520 and RF transmitting section 534. A resistor 521 protects the battery from a dead short if neither a positive nor a negative trace is cut on one of the encoder trinary-input coding pins. A clock-adjust resistor 531, coupled to encoder 529, controls the width of all output pulses.

An output drive resistor 533, coupled to encoder 529, passes drive current to the base of the remote-control transmitter's RF oscillator transistor 543. RF transmitting section 534 comprises a Colpitts oscillator that includes capacitors 535, 541, 537, and 547, a transistor 543, an emitter resistor 545 and inductors 549 and 551. Inductor 549 acts as a power supply decoupler while inductor 551 acts as the printed circuit board antenna loop. Said antenna loop is the source of the RF signal generated by remote-control transmitter 25. A capacitor 553 is provided as a power-supply RF de-coupling capacitor.

Receiver 33, of the super-regenerative type, as shown in FIG. 3 includes a local RF oscillator 419 section, comprising a tuning capacitor 427 and an inductor 435 that are driven by a transistor 437. The encoded RF signal is received through antenna 31, which may be a length of wire approximately one-half wavelength long. It is then AC-coupled by capacitor 415 to the emitter of the common base amplifier 399. This common base amplifier acts as an impedance-matching circuit for the antenna input and as an RF decoupling isolator for the local super-regenerative oscillator to minimize RF feedback into the antenna. Capacitor 413 couples the amplified RF signal from the input amplifier 399 to oscillator 419. Oscillator 419 actually includes two coupled oscillators; a low-frequency oscillator (capacitor 431 and inductor 439) that sweeps the high-frequency oscillator (capacitors 427 and inductor 435) over a wide range of frequencies via coupling capacitor 429. The low-frequency oscillator is referred to as a quenching oscillator and also the quenching signal is sometimes injected from an external oscillator. An on-frequency RF signal injected into the high-frequency oscillator through input capacitor 413 causes the oscillator to go into oscillation prematurely, causing a change in duty cycle of the low-frequency quenching oscillator. This duty-cycle shift is detected at emitter resistor 441 and DC-coupled through resistor 445 to an RF filter capacitor 451 located in an amplifier 444, which filters out the high frequencies of both local oscillators, leaving a digital pulse train identical to that generated by encoder 520 in remote-control transmitter 25 except for amplitude.

A resistor 453 and a capacitor 465 further filter the pulse train to provide automatic gain control (AGC) reference to an operational amplifier 463. An input resistor 449 and a feedback resistor 461 establish the gain of amplifier 463. The output of amplifier 463 is then AC-coupled via a capacitor 469 to an amplifier 458, which is set up as a

5,534,845

9

Schmitt trigger, in that any signal at the input exceeding a predetermined reference level causes a rail-to-rail shift at output 67. The receiver output signal at output 67 is now ready for decoding to see if it is a valid control signal.

Output from receiver 33 is then fed to an RF input 67 of controller 35, as shown in FIG. 2A, for decoding to determine if the input is a valid control input. To establish validity, controller 35 must compare the input with the previously programmed remote-control transmitter 25 codes stored in EEPROM 37. Controller 35 in this case comprises a National Semiconductor COP880 microcontroller with read-only memory (ROM) and random access memory (RAM). If controller 35 receives a valid control signal, it responds to this signal by generating an output or outputs according to the control signal received, the operational mode of controller 35, and the status of the other inputs at the time the signal is received.

As shown in FIGS. 2A and 2B, the security system inputs are indicated at 69, 79, 89, 121, 131, 141, 151, 171, 191, 193, 197 and 203, and each input is buffered by its own individual input buffer circuit. For example, for input 69 (sensor "lock" in FIG. 1) the buffer circuit comprises an isolation resistor 71, a filter, a capacitor 73, an isolation diode 75, and a pull-up resistor 77. All other inputs have similar filters, depending on their application as is known in the art. Examples of these sensor elements are shock sensors; field-disturbance sensors (radar); door, hood, trunk, or ignition switches; audio discriminators (glass-break) sensors; and light sensors.

When the security system is armed, and at other times as required, all the inputs are continually monitored as to the status of the inputs or the change thereof. Some inputs are assigned to various zones for convenience in monitoring the specific areas of the vehicle such as sensors, doors, hood or trunk, etc. These inputs are buffered for voltage transients and surges depending upon the type of input. For example, positive triggered inputs are the positive door circuit FIG. 2B 171, the ignition input 151, and the light sensor input 197/203. The sensor inputs 69, 79, and 89, valet 121, instant (hood/trunk) 131, and negative door 141 are triggered by negative inputs. The valet input comes from depressing a dash-mounted valet switch 122. The wiper input 193 is programmable positive or negative by use of a jumper pin shorting connector at the input selection connector 349. The fact that all these inputs go independently directly to controller 35 allows it to monitor the status of each input separately, as well as to be able to independently disable unstable inputs, and allows for maximum security with the balance of the inputs when any one input becomes unstable and is disabled. This greatly enhances the capability of the advanced self-diagnostics to help maintain the maximum security possible when inputs become unstable.

The security system further includes multiple audio, visual, and electronic output devices. These are indicated in FIGS. 2A and 2B at 107, 233, 235, 269, 281, 291, 305, 313, 321, 329, 337, and 345. Examples of these output devices are sirens (either electronic or mechanical) or synthesized voice outputs 233 and 235, lights (head, running, and dome) 281, door actuators (locking/unlocking motors) 269, device enabled 313 (while the system is armed), trunk-release solenoid 281, dash mounted LED 107 (red/green), starter disconnect 305, horn 345, a remote pager, an autodailer, window roll up/down motors or other control modules, such as remote car-start module, and other vehicle security system sensors. Any auxiliary output channel can be used to control other electrically controlled devices as required by the user.

10

As shown in FIGS. 2A and 2B, all the outputs are generated by controller 35, but well-buffered by the different output devices, depending on the output in question. The power output from controller 35 is buffered by a power inverter 225. It is used to minimize the standby power drain of output power amplifier 263. This power amplifier 263 is a push-pull amplifier with current limiting and thermal shutdown that drives an output speaker connected between outputs 233 and 235 with synthesized voice audio signals from a voice synthesizer 239 or a synthesized siren sound audio signals from six-tone siren synthesizer 257. The lock and unlock control signals are inverted by power invertors 267 and 265 respectively and sent to a three-pin door-lock control connector 269 via printed circuit board conductors that are not numbered in any of the Figures. A five-pin relay drive connector 281 receives its control signals from invertors 273, 275, 277, and 279 to drive control relays in an external module for auxiliary channel 2, running lights, dome lights and headlights. Four more auxiliary output channels and three other outputs are driven by output power transistors and provided with relay kickback protection diodes. They are channel 3 at output 291, starter disconnect at output 305, ground when armed at output 313, channel 4 at output 321, channel 5 at output 329, channel 6 at output 337, and horn at output 345. LED 107 visual outputs, either red or green or both red and green, will give a visual indication of the status of the security system at all times.

A connector at 191 is used for enabling/disabling the radio frequency remote-control transmitter 25 program mode of controller 35. The jumper must be removed to program the system's remote-control transmitters.

The clock speed of the microcontroller is 10 megahertz and is established by quartz crystal 103, capacitors 99 and 101, and a resistor 105. Controller 35 clock, in conjunction with controller 35 program, establishes all of the system's timing.

The controller reset is generated by an active reset circuit consisting of resistors 49, 51, 55, and 61; transistors 57 and 59; diodes 53 and 65; and capacitor 63. When the 5-volt supply voltage drops below 4 volts, the reference at the base of transistor 57 drops below the required transistor turn-on voltage, which causes transistor 57 to turn off. When transistor 57 turns off, it removes the ground at the base of transistor 59, allowing the pull-up resistor 55 to pull-up the base of transistor 59, which turns on transistor 59, generating a reset.

The 12.6 volts DC power for control module 29 enters at 295 and the ground return exits at 299. A ceramic disc capacitor 297 is provided as a radio-frequency filter capacitor located at the power input. A diode 285 is provided as a reverse-protection power diode. Capacitors 229 and 221 are provided to act as a power-supply regulator pre-filter and post-filter respectively. A voltage regulator 223 is provided and preferably is a 5-volt micro power, 100-milliampere regulator. Ceramic disc capacitor 217 and the ferrite beads 215 and 219 are provided on the power traces of controller 35 to reduce radio frequency emissions therefrom which aids in maximizing the range of on-board RF receiver 33.

The first alternate embodiment of the soft-chirp feature is shown in FIG. 2C and shows that during chirps, the siren output 359 would be pulsed at a low-duty cycle rate, and a resistor 361 would limit the current of the pulses as the power is stored in a capacitor 363. A base drive resistor 365 is provided to limit the current from the limited power stored in capacitor 363 to the point that transistor 369 only pulls the input to base drive resistor 367 to, for example, a +10 volts

5,534,845

11

instead of ground. Base drive resistor 367 input only being pulled to +10 volts supplies a very limited current to siren output transistor 371, which then only supplies a very limited current to siren output 373. This limited output current may only generate a voltage of, for example, 2 volts across the siren, which would significantly reduce the output volume of the siren chirps. During normal siren output, the output at 359 would be on continuously, supplying a hard drive to pre-drive transistor 369, which in turn would supply a hard drive to siren output drive transistor 371, which would then supply sufficient current to develop a full 12 volts across the siren, which would develop a full-siren volume.

A second alternate embodiment is shown in FIG. 2D and uses a separate output 375 from controller 35 to supply a limited drive to the siren output drive transistor 371. The output 375 from controller 35 would be on continuously during chirps. Base drive resistor 377 would then deliver current from the output 375 to turn on hard chirp pre-drive transistor 381. In this case, the base drive resistor 379 would be chosen to limit the drive current supplied to the siren output transistor 371, such that the current supplied to the siren would be limited significantly, producing a chirp of a much lower volume. Another embodiment for generating a soft chirp would be to use the alternate routing of the printed circuit board conductor as shown in FIG. 2D in dotted line. In this case, the limiting of the output power would be accomplished by choosing the appropriate value of base drive resistor 377. Using a large-value resistor at 377 would limit the base drive current to the chirp pre-drive transistor 381 so that the voltage at the input to base drive resistor 367 would be, for example, 10 volts. This would limit the base drive current available to siren output drive transistor 371, thereby reducing the output current to the siren, which would produce a reduced-volume chirp.

The security system of this invention is comprised of a number of important new features and functions. The first such feature is the "silent" mode as shown in FIGS. 5A and 5B. The silent mode is the deletion of the siren chirps or synthesized voice that normally accompany the arming or disarming of the vehicle security system. As is well-known in the art, most of today's radio-frequency remote-controlled vehicle-security systems acknowledge the confirmation of the arm/disarm commands with siren chirps, synthesized voice output and light flashes. Most of these security systems have the capability to permanently disable the audio portion of the acknowledgments by use of program switches, jumpers, or changes in the system's operating program. A few security systems have the capability to selectively disable these audio acknowledgments via the RF remote-control transmitter, but in all those instances, something is lost in the process. One such security system uses an auxiliary remote-control channel to disable the audible acknowledgment, but loses the use of that channel for other functions. Another uses a single remote-control transmitter channel, but the audible acknowledgment is delayed until a second signal is transmitted on the same channel and received. In this case, however, the delay becomes a nuisance to the user, and, further, if the first signal is not received, the second signal could be received as a first signal and cause the audible arming notification signal to be generated.

The method of selectively deleting the audio acknowledgment while using the RF remote-control transmitter 25 to arm and disarm the vehicle security system in this invention eliminates both of these shortcomings. The programmed channel 2 of this invention has a built-in channel-confirma-

12

tion delay before the output pulse is generated. The channel 2 output is normally used for trunk release and has a built-in 2.5-second delay to prevent inadvertent release of the trunk. To silence the audible acknowledgments, the user presses channel 2, causing controller 35 to look for a channel 1 input within the next 5 seconds. Upon receipt of this channel 1 input, controller 35 will delete all audible acknowledgments of arming/disarming. The invention requires no loss of an auxiliary channel or the inconvenience of not having immediate acknowledgment of arm/disarm control signals.

Referencing FIGS. 5A and 5B, when controller 35 confirms an input from remote-control transmitter 25 channel 2, at 601, a time check is then made at 603 to determine if controller 35 should generate the trunk-control pulse or start the chirp-delete period. If channel 2 validity is confirmed for two and one half seconds, controller 35 proceeds to 605 to generate a trunk-control pulse to unlock the trunk. If not, controller 35 proceeds to 607, where the five-second audible acknowledgment deletion timer is started, then to 609 where the deletion flag is set. Thereafter, controller 35 returns to the normal operating mode to wait for other events to occur. If a security system arm/disarm command (from channel 1) is confirmed at 615 at this time, when controller 35 checks the audible acknowledgment (chirp) flag and finds it set at 617, controller 35 will bypass generating the audible acknowledgments at 619. When the deletion timer runs down to zero, an interrupt will be generated. When it is determined that the interrupt is a deletion timer interrupt, the interrupt processing routine at 611 is entered where the audible acknowledgment (chirp) deletion flag is reset at 613.

Another feature of the invention is the addition of three new sensor-input capabilities when the security system is armed: warn-away-only sensor input, dual level/warn-away with full-alarm trigger-sensor input, and a two-step door input. In the warn-away only sensor input, the warn-away-only input will not activate the full alarm mode of the security system, but on each new occurrence of the input will generate several seconds of siren chirps or synthesized voice output. This greatly reduces the nuisance of the security system for users who like their sensors highly sensitive. In the case of a field-disturbance sensor set at or near maximum sensitivity, the warn-away sensor input can generate several seconds of warn-away audible outputs if someone comes too near the vehicle even without touching it. Several seconds of chirps or synthesized voice is less of a nuisance than a full duration of the security system full-alarm mode.

In the dual level/warn-away with full-alarm trigger-sensor input, the dual-level sensor input will generate just the warn-away audible output the first time it is activated. If another activation of this sensor input occurs within about 10 seconds, it will trigger the full alarm mode of the security system; if not within the 10 seconds, it will trigger only the warn-away audible output. In the two-step door input feature, upon opening the door, controller 35 generates several seconds of chirps or voice warn-away after which controller 35 will move to the full alarm mode unless it is disarmed by the user using the transmitter 25.

The warn-away, dual-level, and two-step features are depicted in FIGS. 6A-6C and show the microcontroller operations of these functions. If the warn-away input is activated at 631, controller 35 proceeds to generate several seconds of siren chirps or synthesized voice at 633, after which it returns to the normal armed mode. When the dual-level sensor is activated at 621, controller 35 checks to see if the input has been activated in the last 10 seconds at 623. If the input has been activated in the last 10 seconds, the

5,534,845

13

security system enters the full-alarm mode at 629, after which it returns to the normal armed mode. If the input had not been activated within the last 10 seconds, the 10-second timer at 625 is started and controller 35 goes into the warn-away mode and generates several seconds of siren chirps or synthesized voice output at 627, after which controller 35 returns to the normal armed mode.

The two-step door input feature is shown in FIG. 6C. When the input is activated at 637 by opening a door, controller 35 generates several seconds of siren chirps or synthesized voice output at 639. Controller 35 will always go into full alarm mode at 645 if controller 35 is not disarmed at 643 by transmission from remote-control transmitter 25 on channel 1 at 641.

The next innovative feature of the invention, termed the "Nite-Lite" is shown in FIGS. 7A-H. The Nite-Lite feature uses a light sensor, such as a photoresistor, mounted on the dash panel. It is used to measure the level of the available light so that controller 35 may control the lights of the vehicle under various circumstances. Further, controller 35 controls the lights of the vehicle under entirely different circumstances. With respect to the light sensor used to control the lights as it relates directly to the security system, FIG. 7A shows the basic function of the "Nite-Lite". When the security system is armed or disarmed, day or night, controller 35 flashes the running lights one to four times upon receipt of the transmission from remote transmitter 25 channel 1. When the security system enters full-alarm mode during daytime, controller 35 flashes the running lights for the duration of the alarm condition. When the security system is armed at night, the headlights and running lights are turned on for 20 seconds; when the security system is disarmed, the headlights and running lights are turned on for 20 seconds or until the ignition is turned on, and the dome light is turned on for 60 seconds or until the ignition is turned on. During the full-alarm mode at night, the headlights are turned on and the running and dome lights are flashed for the duration of the alarm condition.

When the user is driving the vehicle, the light sensor will turn on the headlights and running lights at a predetermined lower light level after a predetermined delay, and turn them off at a predetermined higher light level after a predetermined delay. Also, when the vehicle windshield wipers are turned on in daytime, even in the intermittent mode, after a predetermined delay, the headlights and running lights will be turned on. At night, if the headlights and running lights are on (system was just disarmed) when the user enters the vehicle and the ignition is turned on, the lights will go out for five seconds to allow for cranking of the engine, then turn back on. Under control of the "Nite-Lite", and the vehicle is being operated with the lights on, when the ignition is turned off, the lights will go off for five seconds and then come back on and remain on for 20 seconds to allow for safe egress from the vehicle. If the lights remain on when the ignition is turned off, this draws attention to the user to turn off the light switch.

Other features of the Nite-Lite include a system light sensor 198 and an override switches 200 and 204 in both directions. They are two single pole switches connected to wires 199 and 201 in one position and 197 and 203 in the other position. Light sensor 198 is in series with switch 200. Actuating switch 204 (connecting 201 and 203) causes controller 35 to interpret the input as daytime; deactuating switch 200 (disconnecting 198 from wire 197) causes controller 35 to interpret the input as night time. "Safe-Lite" is the name given to the open or always-night characteristic of the Nite-Lite feature of the invention, but it can still use the

14

light sensor to determine whether it is day or night. Safe-Lite provides for safer driving since the headlights and running lights will always be on when the vehicle is being driven (the ignition is on). Another feature of the Safe-Lite when linked with the light sensor is to connect the headlights in series during the day time, as an energy-conservation measure, while continuing to run them in parallel at night to obtain maximum brightness.

In FIG. 7A, if the ignition is not on at 667, controller 35 goes to the Nite-Lite ignition-off routine at 669, reference FIG. 7B. If the ignition is on at 667, controller 35 checks to see if there has been a light-level threshold change at 671 and, if there has, controller 35 proceeds to the Nite-Lite light intensity routine at 673, reference FIG. 7C. If no change has been recorded, controller 35 proceeds to check if it is day or night at 675. If it is night, controller 35 proceeds to check if ignition has just been turned on at 683. If it has, controller 35 turns off all lights at 685, starts a five-second "ignition on" timer at 687, and returns to the main program. If at 675, it is day time, controller 35 checks for wiper or Safe-Lite at 677 and proceeds to the appropriate wiper 679, reference FIG. 7D, or Safe-Lite 681, reference FIG. 7G, routine.

If the ignition is off at 667 in FIG. 7A, the security system proceeds to the ignition-off routine 669, as shown in FIG. 7B. If the ignition has not just been turned off at 689, controller 35 goes to the security routine 691, reference FIG. 7E. If the ignition has just been turned off at 689, controller 35 checks to see if it is day or night at 693, daytime, controller 35 returns to the main program; otherwise controller 35 turns off the headlights and running lights at 695, and starts a five-second ignition-off timer at 697, before returning to the main program.

If the ignition has been on for a measurable period, when the "Nite-Lite" routine is entered, controller 35 proceeds to 673, as shown in FIG. 7C, where controller 35 checks the direction of the change at 707, since it has already been established that a change has occurred. An upward change [it is getting lighter] starts the 30-second lights-off timer at 709 and returns to the main program. A opposite or downward change starts the 30-second lights-on timer at 711 and returns to the main program. Thirty second delays are required to prevent controller 35 from turning the lights on and off every time controller 35 encounters brief periods of light change, such as when the vehicle goes under an overpass, etc.

FIG. 7D represents a basic concept of the windshield-wiper routine. The system will operate with intermittent wipers even if they only operate once ever 15 seconds. In other words, if the light-sensor input goes active for a short period every 15 seconds, controller 35 will register it as a continuous input, keep the lights on or turn them on 30 seconds after the first input. The actual windshield wiper input circuit is as given above, but it is preferable to have a direct windshield wiper input to interface with the program to function as above so the light-sensor circuit will not be affected by the intermittent windshield wiper input function. At 721, controller 35 checks to see if the windshield wipers have just been turned on. If they have, the 30-second Nite-Lite lights-on timer is started at 723, before returning to the main program. If not, controller 35 returns directly to the main program.

The Nite-Lite security system routine shown in FIG. 7E controls the lights according to light conditions at the time a security function occurs. The first check is to see if the security system has been just armed or disarmed at 731. If not, controller 35 proceeds to the alarm routine 733, refer-

5,534,845

15

ence FIG. 7F. If the arming state has just changed, a check is made to determine if the security system was armed or disarmed at 735. In both cases, controller 35 then checks for day or night conditions at 737 and 741. If day conditions, controller 35 returns to the main program, where another routine (not Nite-Lite) flashes the running lights one to four times.

If the security system was just armed at 731/735 and it is night conditions at 737, controller 35 turns on the headlights and running lights at 739, then starts a 20-second lights-on timer at 743 before returning to the main program. If the security system was just disarmed at 731/735 and it is night conditions at 741, controller 35 turns on the headlights and running lights at 745, starts a 20-second lights-on timer at 747, turns on the dome lights at 749, and starts a 60-second dome-light timer at 751 before returning to the main program.

The Nite-Lite alarm routine 733, as shown in FIG. 7F, controls the lights during a full-alarm mode of the security system. Controller 35 rechecks to see if the security system has just gone into the full alarm mode at 759. If no full-alarm mode exists, controller 35 returns to the main program. If a full-alarm mode does exist, controller 35 checks to see if it is day time or night time at 761. In daytime, controller 35 flashes the running lights at 763 for the duration of the alarm. At night, controller 35 turns on the headlights and flashes the running and dome lights at 765 for the alarm duration.

Safe-Lite is the capability of the Nite-Lite feature that turns on the headlights and running lights any time the ignition is turned on. In FIG. 7G, the light sensor allows the Safe-Lite feature to turn on headlights in series at 771 or in parallel at 767, depending on whether it is day or night at 769 respectively.

The Nite-Lite feature requires several timers that all generate interrupts when the time expires. This requires a routine to process these interrupts as shown in FIG. 7H. The first item checked in this routine is whether the ignition is on or off at 775. If it is on, controller 35 checks for on or off timer at 777. An off timer will turn off the headlights and running lights at 779, while an on timer will turn on the headlights and running lights at 781. If at 775 the ignition is not on, controller 35 again proceeds to check to see if it is an on or off timer at 783. The on-timer interrupt turns on the headlights and running lights at 789 and starts a 20-second on timer at 793 before returning to the main program. The off-timer interrupt checks to see if the interrupt is for the headlights and running lights or dome light at 785, and proceeds to turn off the appropriate lights before returning to the main program. At 787 controller 35 turns off the dome lights, while at 791 controller 35 turns off the headlights and running lights.

Another feature of the invention is shown in FIG. 8A and is an advanced input-diagnostic and input-bypass capability in which an unstable input is bypassed (disabled) after starting four full-alarm cycles in one hour. The unstable input is thereafter bypassed for an additional hour from the time of any activation of the input during the one-hour bypass period, and the bypassing can only be terminated by the input remaining stable for one full hour or the security system being disarmed and the ignition being turned on. Each time an input is activated that causes the security system to enter the full-alarm mode, controller 35 goes through a routine that checks the stability of the input for the last one-hour period or starts a check for the next one-hour period.

The input-bypass routine 795, as shown in FIG. 8A, starts by checking to determine if the security system is armed at

16

797. If the system is not armed, controller 35 checks to see if the ignition has just been turned on at 799, and if it has, controller 35 will reset all bypass flags, activation counters and associated timers at 801 before returning to the main program. If the security system is armed at 797, the input activation-counter of controller 35 is incremented at 803 and the count is checked to see if the input has been activated four times in the last hour at 805. If this is the fourth activation, the input-bypass flag is set for this input at 807, the bypass timer is set to one hour and started at 811, then controller 35 returns to the main program without generating an alarm output. If the input was not the fourth activation in one hour at 805, controller 35 checks to see if the bypass flag has been previously set at 809. If it has been set, controller 35 proceeds to 811. If the flag is not set at 809, controller 35 checks to see if the input-bypass activation timer is running at 813. If it is not, it means this is the first activation of this input. Controller 35 then proceeds directly to 819, where the input-bypass activation timer is reset to zero and started. Thereafter, controller 35 proceeds to the full-alarm mode at 821. If the timer is running at 813, a check is made to see if the timer is above or below one hour at 815. If it is above one hour, this input has not triggered in the last hour, so the activation counter is set to "1" at 817 and the timer is reset to "0" and started, before going to the full-alarm mode at 821. If the input-activation timer is below one hour at 815, controller 35 proceeds directly to the full-alarm mode at 821. There is one input bypass timer in controller 35 for each input that has been activated. If an input-bypass timer decreases ("decrements") to zero, an interrupt is generated, causing controller 35 to go to the bypass-timer interrupt processing routine at 827, as shown in FIG. 8B. This resets the input-bypass flag for the appropriate input at 829, then returns to the main program.

Another feature of the invention is the capability of putting the security system into and out of "valet" mode by using transmitter 25 and one of the vehicle's doors, as shown in FIG. 9. This simplifies the entry and exit of "valet" mode for the user. The security system still has the capability to enter or exit "valet" using the dash mounted system valet switch when the ignition is on.

The routine begins at 833 and, as shown in FIG. 9, by disarming the security system at 835, opening a door of the vehicle at 839; and confirming receipt of a signal from security system remote-control channel one at 837. Then, within two seconds at 845 and 849, confirming receipt of a transmission from security system remote-control channel two at 847, and again within two seconds at 851 and 855 confirming receipt of a transmission from remote-control channel one at 853. Controller 35 toggles the valet function at 859. During the process, controller 35 will always toggle into the arm mode at 843. If at any time during this operation the constraints specified above are not met, controller 35 will toggle between the security system arm/disarm modes at 841 and 857.

Programming one of the security system's auxiliary control channels [channel 3], to operate a remote car-start module, is another of the invention's features and is shown in FIGS. 10A-C. This capability is enabled or disabled when the system operational functions are programmed. By customizing channel 3 to be used as a remote car-start output channel, the security system can disable the sensor inputs (radar, shock, motion, etc.) while maintaining a significant level of security by keeping all the other inputs active when the security system is in the armed mode.

In car start routine 871, when receipt of remote-control transmitter 25 channel 3 is confirmed at 873, controller 35

5,534,845

17

checks to see if channel 3 has been programmed for car-start mode at 875. If it has not, the auxiliary channel 3 output is turned on for the duration of the control-channel confirmation at 877 (as long as the remote-control transmitter 25 button is depressed), before returning to the main program. 5 If remote-control transmitter 25 channel 3 is programmed for car start, then the car-start flag is set at 879 and a check is made to see if the security system is armed at 881. If the security system is not armed, the doors are locked at 883, channel 3 output is turned on for the duration of channel 10 confirmation at 887, and the car start disarmed flag is set at 891 before returning to the main program. If at 881 the security system is armed, controller 35 turns on channel 3 output for the duration of the transmission of remote-control transmitter 25 channel three confirmation at 885, sets bypass 15 flags for sensor inputs one and two at 893, then sets channel three car-start armed flag at 895 before returning to the main program.

In the channel 3 car start disarmed flag routine 903, as shown in FIG. 10B, when receipt of a transmission of remote-control transmitter 25 channel one is confirmed at 20 905 and the channel three car-start flag is on at 907, the security system unlocks the vehicle's doors, resets the car-start disarmed flag and the car-start flag at 911, before returning to the main program; otherwise channel 1 operations are normal for the main remote-control transmitter 25 channel 1, at 909. In the channel 3 car start armed flag routine 917, as shown in FIG. 10C, with the car-start armed 25 flag set when receipt of remote-control transmitter 25 channel 1 is confirmed at 919 and the channel 3 car-start flag is on at 921, controller 35 resets sensor one and two bypass 30 flags at 925, disarms the security system, unlocks the vehicle's doors, and resets the car-start-armed flag and the car-start flag at 927, before returning to the main program; otherwise, channel 1 operations are normal at 923.

Another feature of the invention allows all system-programmable operational functions to be selected using the security system remote-control transmitter 25. Function programming is shown in FIG. 11 and is accomplished by using the security system's normal inputs (door, ignition, 40 and valet) to put the security system into the function programming mode, then using the security system's remote-control transmitter 25 to toggle the operational function to the desired state.

In FIG. 11, the security system must be disarmed at 993, 45 the doors closed at 995, and the ignition must be off at 997 to initiate the sequence required to begin entry into the security-system operational-function programming mode. The ignition must then be turned on at 999 and the valet switch must be pressed once at 1001 to enter the operational-function programming mode at 1003. At this time, the state of the first operational-function can be toggled at 1007 using 50 remote-control transmitter 25 at 1005. If the user does not desire to change the state of this function, he or she may advance to the next selected function by depressing the valet 55 switch once for each function at 1015. There are only two states of any function, a factory-default state and an alternate state. Accordingly, one chirp denotes the factory-default state, while two chirps denote the alternate state. At any time a particular function is selected, that function's state can be 60 toggled by using remote-control transmitter 25 at 1015 or not toggled by pressing the valet switch to advance the operational function selection to the next in the sequence. At any time, the user can exit the operational-function programming mode by turning on the ignition at 1017, opening 65 a door at 1019, or stepping through the balance of the programmable operational-functions at 1021.

18

The next new feature of the security system, the "test mode" is shown in FIGS. 12 and will be a great aid to the security-system installer. This feature allows the installer or the user to conduct a complete test of all of the security system's inputs, including inputs from remote-control transmitter 25. Access to this test mode is somewhat involved, but the steps are necessary to prevent inadvertent entry which would eliminate the security of the security system. In this test mode, the user may choose any input for testing and the security system will respond with a siren chirp when the input goes active, and another siren chirp when the input goes inactive. At the same time, the security system's light-emitting-diode, LED 107, will indicate the last two inputs (zones) activated.

As shown in FIGS. 12A, 12B and 12C to enter the security-system test mode, the security system must be disarmed at 1027-9. Valet switch 122 must then be pressed and held at 1031, the ignition turned on and off at 1033, valet switch 122 released at 1035, and pressed and released again at 1037. Controller 35 then enters the test mode at 1041 and acknowledges with a long siren chirp at 1039. While in the test mode, any input may be checked at any time until receipt of a transmission from remote-control transmitter 25 channel 1 is confirmed at 1077. Thereafter, any particular input may be selected by depressing the channel 1 button on transmitter 25 the number of times corresponding to the number of that input. Examples of input testing are shown in FIGS. 12A and 12B by numbers 1043-1071.

For example, when the door is opened at 1043, the siren chirps once to acknowledge the door-open input going active and LED 107 flashes twice at 1045, to indicate that it is a zone 2 input. LED 107 will continue to flash twice at 1045, with a short pause between groups of flashes to continue to indicate that zone 2 was the zone from which the last two inputs came. When the door is closed at 1047, the input goes inactive; and at 1049 controller 35 acknowledges the door going inactive with another siren chirp, while LED 107 continues its flashing at 1051. LED 107 will continue to flash as above until another input is activated at 1055 or the ignition is turned on at 1053, at which time controller 35 will exit the test mode and return to the main program.

In another example, after the door input is tested, the hood or trunk is physically opened, activating zone three at 1055. The siren chirps once to acknowledge the input going active and LED 107 flashes 3 times (indicating zone 3), pauses, flashes twice at 1057 indicating that the previous input was from zone 2. When the hood or trunk is closed at 1059, the input goes inactive, controller 35 acknowledges the input going inactive with another siren chirp, while the LED 107 continues to flash as above at 1061. Again the LED will continue to flash as above at 1063 until another input goes active at 1067 (zone 4 acknowledged by chirps at 1069 and zone identification displayed at 1071) or 1075, or the ignition is turned on at 1053, 1065, 1073 or 1083, which in these instances will cause controller 35 to exit the test mode.

If at 1077 receipt of a transmission from transmitter 25 channel 1 is confirmed for a selected number of times, that selected zone and only that selected zone can be tested at 1079. A major feature of the security system test mode is the capability to test the range of the transmitter 25 by using any of the channels except channel 1. While in the test mode, if any of the auxiliary channel inputs are confirmed at 1081, the siren will chirp once a second at a test loop comprising 1081, 1085, and 1087 for as long as the input channel is confirmed at 1081. This allows the installer or user to walk away from and around the vehicle to test the range of transmitter 25 without operating any of the security system's

5,534,845

19

functions except for the chirping siren. If the installer or user notices a loss in chirping while in any specific location around the vehicle, control module 29 may be moved to a new location or an extender antenna may be added to increase the transmitter range.

Another feature of the invention is the capability of the security system to restart itself after a power failure to the same conditions in effect when the power failure occurred. In FIG. 13, at power-down at 1093, controller 35 checks for the initiation of its reset function at 1095. If controller 35 has just entered reset, it stores the program counter at 1097, and the operating registers (in RAM) at 1099 in permanent memory, before halting the program. In FIG. 15, when power is restored at 1107, the operating registers are restored at 1109 and the program returns to the point it was operating when the power failed at 1111 and 1113.

The last feature of the invention is the capability of the security system to lower the volume of the chirps. As shown in FIGS. 14 and 16, these chirps may either be "softened" at 1121 using transmitter 25 or programmed for softer operation during system operational function programming. As the pulse width of the power pulses is diminished, the power-output (volume) of the siren is likewise diminished. This is shown in FIG. 14 where the reduction is set at 90% (a 10% duty cycle).

In FIG. 14A, a 100-microsecond timer is started at 1123, the siren output is turned on at 1125, and the program enters a loop until the 100 microseconds have expired at 1127. When the 100 microseconds expire, the siren-off timer is set to 900 microseconds at 1129 and the siren is turned off at 1131, before controller 35 returns to the main program.

In FIG. 16, when the siren-off timer decrements to zero an interrupt is generated at 1135, the main chirp timer is decremented at 1137, and checked for a value of zero at 1139. If the timer is at zero, controller 35 returns to the main program, but if it is not at zero, the soft chirp 1121 continues.

Another means of softening the chirps is shown in FIGS. 2B and 2C where the output transistor base drive current is reduced thereby providing a lower output voltage to the security system siren. This latter method may be accomplished in two ways: the output of controller 35 may be pulsed during chirping to a holding capacitor, thereby reducing the output transistor drive current (FIG. 2C), or a separate controller output may be used to drive the siren output transistor (FIG. 2D).

What is claimed is:

1. An electrically powered security system for monitoring and controlling access to a protected area and having multiple levels of alert signal commensurate with the level of security threat to the area, comprising:
 - a) a plurality of sensor input devices located about the protected area, for providing input corresponding to the level of security threat to the area;
 - b) means for communicating multiple levels of alert signals, both visual and audible, commensurate with the level of threat received to the area, including:
 - (i) a low level alert consisting of a voice warnaway, series of audible chirps or blinking lights;
 - (ii) a medium level alert consisting of a combination of said voice warnaway, series of said audible chirps and said blinking lights; and,
 - (iii) a high level alert consisting of an immediate full siren alert and said blinking lights, wherein said audible siren alert is generated by a voltage at a siren;
 - c) means for permanently storing system operational parameters within an electrically programmable and erasable read-only memory; and,

20

d) a controller for using said operational parameters for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said input devices and causes said means for communicating to issue said multiple levels of alert signals of a level commensurate with and in response to said sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:

- (i) means for detecting a sensor input signal corresponding to each said level of threat to the secured area;
- (ii) means for generating an output signal to said means for communicating said level of alert corresponding to said sensor input signal; and,
- (iii) means for generating an additional output signal to said means for communicating said level of alert upon receipt of additional input signals from said sensors either at the same or higher threat level or within a set period of time following receipt of first said sensor input signal.

2. An electrically powered security system for monitoring and controlling access to a protected area and having a capability of selectively deleting audible alert signals following arm/disarm mode change, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible;
- c) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver; and,

d) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:

- (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
- (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
- (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
- (iv) means for selectively changing audible and visual alert signal to an audio free, visual only alert signal upon receipt of a first control signal transmitted from one channel of said transmitter to said receiver and thereafter receipt of a second control signal transmitted from another channel of said transmitter within a set time period so that said two transmission channels are thereafter available for other programmed functions.

3. An electrically powered security system for monitoring and controlling access to a protected area and having a manual and remote capability of changing the mode of said security system between a security mode and a valet mode, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;

21

- b) means for communicating multiple levels of alert signals, both visual and audible;
- c) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver; and,
- d) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
 - (iv) means for said controller to engage/disengage valct mode upon a user-activated input, decoding and acting upon a transmission of control signals from said transmitter.

4. An electrically powered security system for monitoring and controlling access to a protected area and having a capability of testing the installation of said security system, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert, both visual and audible;
- c) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver; and,
- d) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
 - (iv) means for identifying the last two inputs tested using a visual indicator.

5. An electrically powered security system for monitoring and controlling access to a protected area and having a capability of testing the installation of said security system, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;

22

- b) means for communicating multiple levels of alert signals, both visual and audible;
- c) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver; and,
- d) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
 - (iv) means for testing the range of transmissions from said remote transmitter away from and around the protected area in the form of a periodic chirp issued from said means for communicating said multiple levels of alert signals in response to said transmissions received by said radio frequency and decoded by said controller.

6. An electrically powered security system for monitoring and controlling access to a protected area and having capability in a controller for monitoring and analyzing each sensor input for stability, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible;
- c) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver;
- d) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver; and,
- e) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
 - (iv) means for bypassing said sensor input found to be unstable for a period of time, and means for con-

5,534,845

23

tinuing to analyze all said inputs, including bypassed inputs, and returning said bypassed input to said security system when later determined to have regained stability.

7. An electrically powered security system for monitoring and controlling access to a protected area and having capability in a controller for monitoring and analyzing each input for stability, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible;
- c) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals;
 - (iv) means for bypassing said sensor input found to be unstable for a period of time, and means for continuing to analyze all said inputs, including bypassed inputs, and returning said bypassed input to said security system when later determined to have regained stability; and,
 - (v) means for counting the number of activations from each input that cause the security system to actuate an alarm, over a period of time, in making a determination whether an input has become unstable.

8. An electrically powered security system for monitoring and controlling access to a protected area and having capability in a controller for monitoring and analyzing each input for stability, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals both visual and audible;
- c) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating stimulate multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals;
 - (iv) means for bypassing said sensor input found to be unstable for a period of time, and means for continuing to analyze all said inputs, including bypassed inputs, and returning said bypassed input to said

24

security system when later determined to have regained stability; and,

- (v) means in said controller to readmit said unstable input into said security system only after being determined to have regained stability not withstanding said security system undergoing cycling through said arm/disarm/arm modes.

9. An electrically powered security system for monitoring and controlling access to a protected area and having capability in a controller for monitoring and analyzing each input for stability, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible;
- c) an electrically programmable and erasable read-only memory; and,
- d) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals;
 - (iv) means for bypassing for a period of time an input found to be unstable, and means for continuing to analyze all said inputs, including bypassed inputs, and returning said bypassed input to said security system when later determined to have regained stability; and,
 - (v) means for permanently storing system operational parameters in an electrically programmable and erasable read-out memory and for restoring said security, and upon restoration of power, to the same state as it had when power was curtailed.

10. An electrically powered security system for monitoring and controlling access to a protected area and having capability in a controller for reducing volume of alert siren chirps, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible, including a siren wherein volume of audible siren alert is generated by a voltage at said siren;
- c) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;

5,534,845

25

- (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
- (iv) means in said controller for reducing said volume of siren chirps by effectively reducing the voltage and current at said siren input, includes other means in said controller for reducing said volume of said siren chirps including means for temporarily changing said immediate audible/visual notification signal to an immediate reduced volume audible/visual notification signal upon receipt of a first control signal transmitted from one channel of said transmitter to said receiver and thereafter receipt of a second control signal transmitted from another channel of said transmitter within a set time period so that said two transmission channels are thereafter available for other programmed functions.

11. An electrically powered security system for monitoring and controlling access to a protected area and having capability in a controller for reducing volume of alert siren chirps, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible, including a siren wherein volume of audible siren alert is generated by a voltage at siren input;
- c) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
- (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
- (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
- (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
- (iv) means in said controller for reducing said volume of siren chirps by effectively reducing the voltage and current at said siren input by pulsing said siren input power at a low duty cycle rate.

12. An electrically powered security and convenience system for monitoring and controlling access to a vehicle and having multiple levels of alert signal commensurate with the level of security threat to the vehicle, comprising:

- a) a plurality of sensor input devices located about the vehicle, including such as switches, shock sensors or field disturbance sensors, each for sensing a threatening event and providing a sensor activated input of a level corresponding to the level of security threat to the vehicle;
- b) means for communicating multiple levels of alert signals, both visual and audible, commensurate with the level of threat received to the area, including:
- (i) a low level alert consisting of a voice warnaway, series of audible chirps or blinking lights;
- (ii) a medium level alert consisting of a combination of said voice warnaway, series of said audible chirps and said blinking lights; and,

26

- (iii) a high level alert consisting of an immediate full siren alert and said blinking lights, wherein said audible siren alert is generated by a voltage at a siren;
- c) means for permanently storing system operational parameters within an electrically programmable and erasable read-only memory; and,
- d) a controller for using said operational parameters for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said input devices and causes said means for communicating to issue said multiple levels of alert signals of a level commensurate with and in response to said sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
- (i) means for detecting a sensor input signal corresponding to each said level of threat to the secured area;
- (ii) means for generating an output signal to said means for communicating said level of alert corresponding to said sensor input signal; and,
- (iii) means for generating an additional output signal to said means for communicating said level of alert upon receipt of additional input signals from said sensors either at the same or higher threat level or within a set period of time following receipt of first said sensor input signal.

13. An electrically powered security and convenience system for monitoring and controlling access to a vehicle and having a capability of selectively deleting audible alert signals following arm/disarm mode change, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible;
- c) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver; and,
- d) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
- (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
- (ii) means for generating an output signal to said means for communicating multiple levels of alert signals corresponding to said sensor input signal;
- (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
- (iv) means for selectively changing audible and visual alert signal to an audio free, visual only alert signal upon receipt of a first control signal transmitted from one channel of said transmitter to said receiver and thereafter receipt of a second control signal transmitted from another channel of said transmitter within a set time period so that said two transmission channels are thereafter available for other programmed functions.

14. An electrically powered security and convenience system for monitoring and controlling access to a vehicle and having a manual and remote capability of changing the mode of said security system between a security mode and a valet mode, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible;
- c) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver; and,
- d) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
 - (iv) means for said controller to engage/disengage valet mode upon a user-activated input, decoding and acting upon a transmission of control signals from said transmitter.

15. An electrically powered security and convenience system for monitoring and controlling access to a vehicle and having a capability of switching from stored programming to other operational function programming, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible;
- c) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver;
- d) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals;
 - (iv) means for switching from operational function programming, stored in said electrically program-

mable and erasable read-only memory and initially preset therein, to other operational function programming, using a user activated input, decoding and acting upon receipt of control signals from said transmitter.

16. An electrically powered security and convenience system for monitoring and controlling access to a vehicle and having a capability of testing the installation of said security system, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible;
- c) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver; and,
- d) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said variable alert signal corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
 - (iv) means for identifying the last two inputs tested using a visual indicator.

17. An electrically powered security and convenience system for monitoring and controlling access to a vehicle and having a capability of testing the installation of said security system, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible;
- c) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver; and,
- d) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,

(iv) means for testing the range of transmissions from said remote transmitter away from and around the protected area in the form of a periodic chirp issued from said means for communicating said multiple levels of alert signals in response to said transmissions received by said radio frequency and decoded by said controller.

18. An electrically powered security and convenience system for monitoring and controlling access to a vehicle and having capability in a controller for monitoring and analyzing each input for stability, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible;
- c) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver;
- d) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver; and,
- e) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
 - (iv) means for bypassing said sensor input found to be unstable for a period of time, and means for continuing to analyze all said inputs, including bypassed inputs, and returning said bypassed input to said security system when later determined to have regained stability.

19. An electrically powered security and convenience system for monitoring and analyzing each input for stability, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible;
- c) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;

(ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;

(iii) means in said controller for decoding said transmissions and processing said sensor input signals;

(iv) means for bypassing said sensor input found to be unstable for a period of time, and means for continuing to analyze all said inputs, including bypassed inputs, and returning said inputs, including bypassed inputs, and returning said bypassed input to said security system when later determined to regained stability; and,

(v) means for counting the number of activations from each input that cause the security system to activate an alarm, over a period of time, in making a determination whether an input has become unstable.

20. An electrically powered security and convenience system for monitoring and controlling access to a vehicle and having capability in a controller for monitoring and analyzing each input for stability, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals both visual and audible;
- c) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals;
 - (iv) means for bypassing said sensor input found to be unstable for a period of time, and means for continuing to analyze all said inputs, including bypassed inputs, and returning said bypassed input to said security system when later determined to have regained stability; and,
 - (v) means in said controller to readmit said unstable input into said security system only after being determined to have regained stability notwithstanding said security system undergoing cycling through said arm/disarm/arm modes.

21. An electrically powered security and convenience system for monitoring and controlling access to a vehicle and having a capability in restoring said security system upon restoration of power following a power failure, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible;
- c) an electrically programmable and erasable read-only memory; and,
- d) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor

31

devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:

- (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
- (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
- (iii) means in said controller for decoding said transmissions and processing said sensor input signals;
- (iv) means for bypassing for a period of time and an input found to be unstable, and means for continuing to analyze all said inputs, including bypassed inputs, and returning said bypassed input to said security system when later determined to have regained stability; and,
- (v) means for permanently storing system operational parameters in an electrically programmable and erasable read-only memory and for restoring said security, and upon restoration of power, to the same state as it had when power was curtailed.

22. An electrically powered security and convenience system for monitoring and controlling access to a vehicle and having capability in a controller for reducing volume of alert siren chirps, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible, including a siren wherein volume of audible siren alert is generated by a voltage at said siren;
- c) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
 - (iv) means in said controller for reducing said volume of siren chirps by effectively reducing the voltage and current at said siren input, includes other means in said controller for reducing said volume of said siren chirps including means for temporarily changing said immediate audible/visual notification signal to an immediate reduced volume audible/visual notification signal upon receipt of a first control signal transmitted from one channel of said transmitter to said receiver and thereafter receipt of a second control signal transmitted from another channel of said transmitter within a set time period so that said two transmission channels are thereafter available for other programmed functions.

23. An electrically powered security and convenience system for monitoring and controlling access to a vehicle and having capability in a controller for reducing volume of alert siren chirps, comprising:

32

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible, including a siren wherein volume of audible siren alert is generated by a voltage at siren input;
- c) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
 - (iv) means in said controller for reducing said volume of siren chirps by effectively reducing the voltage and current at siren input by pulsing siren input power at a low duty cycle rate.

24. An electrically powered security and convenience system for monitoring and controlling access to a vehicle and having a capability of providing a remote engine start signal, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible;
- c) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver; and,
- d) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
 - (iv) means in said controller, for receipt of a transmission from said remote transmitter, activates a vehicle starting routine that checks the arm/disarm status of the vehicle security system, bypasses the lowest threat level inputs if the system is in the armed mode, locks the vehicle access doors if the system is in the disarm mode, and then outputs a signal to remote start the engine.

25. An electrically powered security system for monitoring and controlling access to a protected area and having

multiple levels of alert signal commensurate with the level of security threat to the area, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different input levels of security threat corresponding to the level of threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible, progressively including:
 - (i) a low level alert consisting of a voice warn-away, series of audible chirps or blinking lights;
 - (ii) a medium level alert consisting of a combination of said voice warnaway, series of said audible chirps and said blinking lights; and,
 - (iii) a high level alert consisting of an immediate full siren alert and said blinking lights, wherein said audible siren alert is generated by a voltage at a siren;
- c) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver;
- d) means for permanently storing system operational parameters within an electrically programmable and erasable read-only memory; and,
- e) a controller for using said operational parameters for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said input devices and causes said means for communicating to issue said multiple levels of alert signals of a level commensurate with and in response to said sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting a sensor input signal corresponding to each said level of threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said level of alert corresponding to said sensor input signal; and,
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
 - (iv) means for generating an additional output signal to said means for communicating said multiple levels of alert signals upon receipt of additional input signals from said sensors either at the same or higher threat level or within a set period of time following receipt of said first sensor input signal.

26. An electrically powered security and convenience system for monitoring and controlling access to a vehicle and having multiple levels of alert signal commensurate with the level of security threat to the vehicle, comprising:

- a) a plurality of sensor input devices located about the vehicle, including switches, shock sensors or field disturbance sensors, each for sensing a threatening event and providing a sensor activated input of a level corresponding to the level of threat to the vehicle;
- b) means for communicating said multiple levels of alert signals, both visual and audible, commensurate with the level of threat received to the area including:
 - (i) a low level alert consisting of a voice warn-away, series of audible chirps or blinking lights;
 - (ii) a medium level alert consisting of a combination of said voice warnaway, series of said audible chirps and said blinking lights; and,

- (iii) a high level alert consisting of an immediate full siren alert and said blinking lights, wherein said audible siren alert is generated by a voltage at a siren;
- c) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver;
- d) means for permanently storing system operational parameters within an electrically programmable and erasable read-only memory; and,
- e) a controller for using said operational parameters for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said input devices and causes said means for communicating to issue said multiple levels of alert signals of a level commensurate with and in response to said sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting a sensor input signal corresponding to each said level of threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said level of alert corresponding to said sensor input signal; and,
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
 - (iv) means for generating an additional output signal to said means for communicating said multiple levels of alert signals upon receipt of additional input signals from said sensors either at the same or higher threat level or within a set period of time following receipt of said first sensor input signal.

27. An electrically powered security system for monitoring and controlling access to a protected area and having a capability of testing the installation of said security system, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals both visual and audible;
- c) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver; and,
- d) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals;
 - (iv) means for using a siren to generate a chirp, audible in and around the protected area, to indicate the

change of state of a sensor installation from active to inactive and inactive to active; and,
 (v) means for identifying the last two inputs tested using a visual indicator.

28. An electrically powered security and convenience system for monitoring and controlling access to a vehicle and having a capability of testing the installation of said security system, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals both visual and audible;
- c) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver; and,
- d) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals;
 - (iv) means for using a siren to generate a chirp, audible in and around the protected area, to indicate the change of state of a sensor installation from active to inactive and inactive to active; and,
 - (v) means for identifying the last two inputs tested using a visual indicator.

29. An electrically powered security system for monitoring and controlling access to a protected area and having a manual and remote capability of changing the mode of said security system between a security mode and a valet mode, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible;
- c) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver;
- d) said valet mode selectively disengaging, a user defined subgroup of said input sensors; and,
- e) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;

(ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;

(iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,

(iv) means for said controller to engage/disengage said valet mode upon a user-activated input, decoding and acting upon a transmission of control signals from said transmitter.

30. An electrically powered security and convenience system for monitoring and controlling access to a vehicle and having a manual and remote capability of changing the mode of said security system between a security mode and a valet mode, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible;
- c) a radio frequency receiver and antenna for receiving a digitally encoded transmission, a radio frequency remote control transmitter having means for generating multiple digitally encoded control transmission signals to said receiver;
- d) said valet mode selectively disengaging, a user defined subgroup of said input sensors; and,
- e) a controller for controlling the operation of said security system so that said system operates in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating said alert signals, said controller comprising:
 - (i) means for detecting said sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
 - (iv) means for said controller to engage/disengage valet mode upon a user-activated input, decoding and acting upon a transmission of control signals from said transmitter.

31. An electrically powered security system for monitoring and controlling access to a protected area and having a capability in said controller for reducing the volume of the alert siren chirps, comprising:

- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area;
- b) means for communicating multiple levels of alert signals, both visual and audible, including a siren wherein the volume of audible siren alert is generated by a voltage at the siren;
- c) a controller for controlling the operation of said security system so that said system may be operated in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating alert signals, said controller comprising:

5,534,845

37

- (i) means for detecting a sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal; 5
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
 - (iv) means in said controller for reducing the volume of siren chirps by effectively reducing the voltage and current at the siren output by using a separate pre-driver transistor, which is driven by a separate chirp signal independent of the extended siren output, for generating the chirp base drive to the siren output drive transistor. 10 15
32. An electrically powered security and convenience system for monitoring and controlling access to a vehicle and having a capability in said controller for reducing the volume of the alert siren chirps, comprising:
- a) a plurality of sensor input devices located about the protected area, for providing different inputs of security threat corresponding to a threat to the area; 20
 - b) means for communicating multiple levels of alert signals, both visual and audible, including a siren wherein the volume of audible siren alert is generated by a voltage at the siren; 25

38

- c) a controller for controlling the operation of said security system so that said system may be operated in an armed mode wherein said controller monitors said sensor devices and causes said communicating means to issue said multiple levels of alert signals in response to a sensor activated signal, or in a disarmed mode wherein said system is disabled from communicating alert signals, said controller comprising:
 - (i) means for detecting a sensor input signal corresponding to each said threat to the secured area;
 - (ii) means for generating an output signal to said means for communicating said multiple levels of alert signals corresponding to said sensor input signal;
 - (iii) means in said controller for decoding said transmissions and processing said sensor input signals; and,
 - (iv) means in said controller for reducing the volume of siren chirps by effectively reducing the voltage and current at the siren output by using a separate pre-driver transistor, which is driven by a separate chirp signal independent of the extended siren output, for generating the chirp base drive to the siren output drive transistor.

* * * * *

US005646591A

United States Patent [19]

[11] **Patent Number:** 5,646,591

Issa et al.

[45] **Date of Patent:** Jul. 8, 1997

[54] **ADVANCED METHOD OF INDICATING INCOMING THREAT LEVEL TO AN ELECTRONICALLY SECURED VEHICLE AND APPARATUS THEREFOR**

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,584,569 4/1986 Lopez et al. 340/429
 4,866,417 9/1989 DeFino et al. 340/429
 5,084,697 1/1992 Hwang 340/566

[75] **Inventors:** Darrell Issa; Jerry Birchfield, both of Vista, Calif.

Primary Examiner—Glenn Swann
Attorney, Agent, or Firm—Sam Talpalatsky

[73] **Assignee:** Directed Electronics, Inc., Vista, Calif.

[57] **ABSTRACT**

[21] **Appl. No.:** 468,703

A method of indicating a degree of incoming threat to an electronically secured area consists of the steps of sensing via sensor a degree of threat delivered to a secured area and generating an electric signal proportional to the degree of threat; analyzing the signal to determine if it is a low degree of threat or a high degree of threat; and producing either a first pulse representing low degree of threat or separately producing the first pulse and a second pulse representing a signal having both low degree of threat and high degree of threat.

[22] **Filed:** Jun. 5, 1995

Related U.S. Application Data

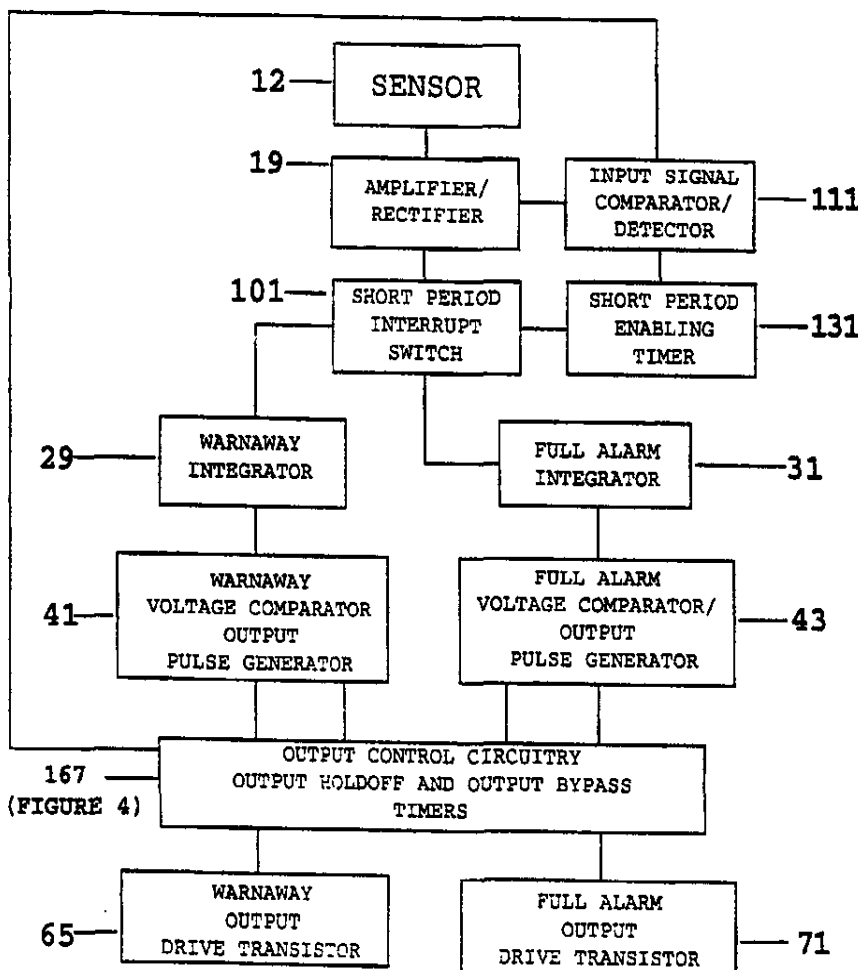
[63] Continuation-in-part of Ser. No. 945,667, Sep. 16, 1992, Pat. No. 5,534,845, and Ser. No. 433,819, May 4, 1995, abandoned, which is a continuation-in-part of Ser. No. 112,940, Aug. 30, 1993, Pat. No. 5,532,670, which is a continuation-in-part of Ser. No. 886,871, May 22, 1992, abandoned.

[51] **Int. Cl.⁶** G08B 13/22

[52] **U.S. Cl.** 340/566; 340/429

[58] **Field of Search** 340/429, 566

94 Claims, 15 Drawing Sheets



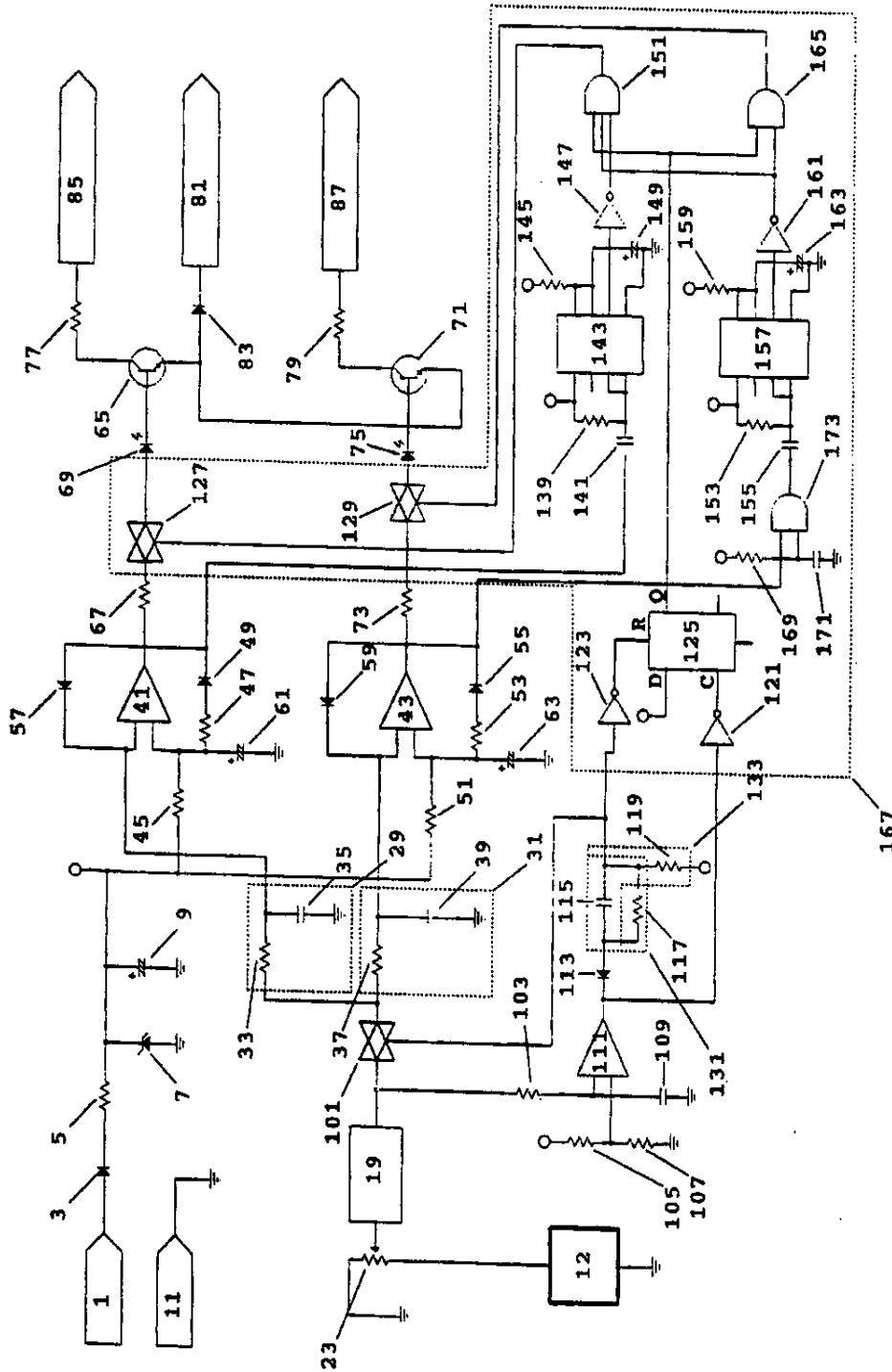


FIGURE 1

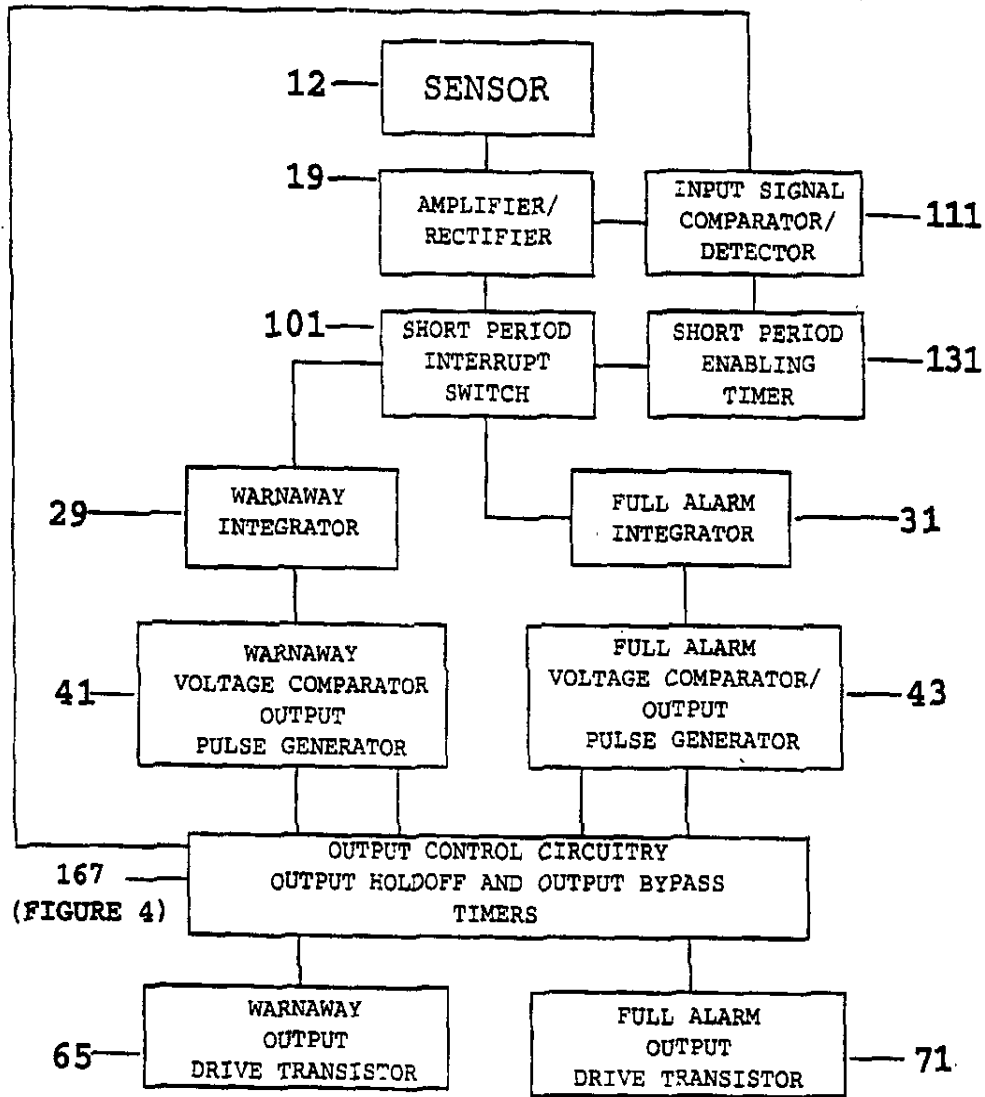


FIGURE 2

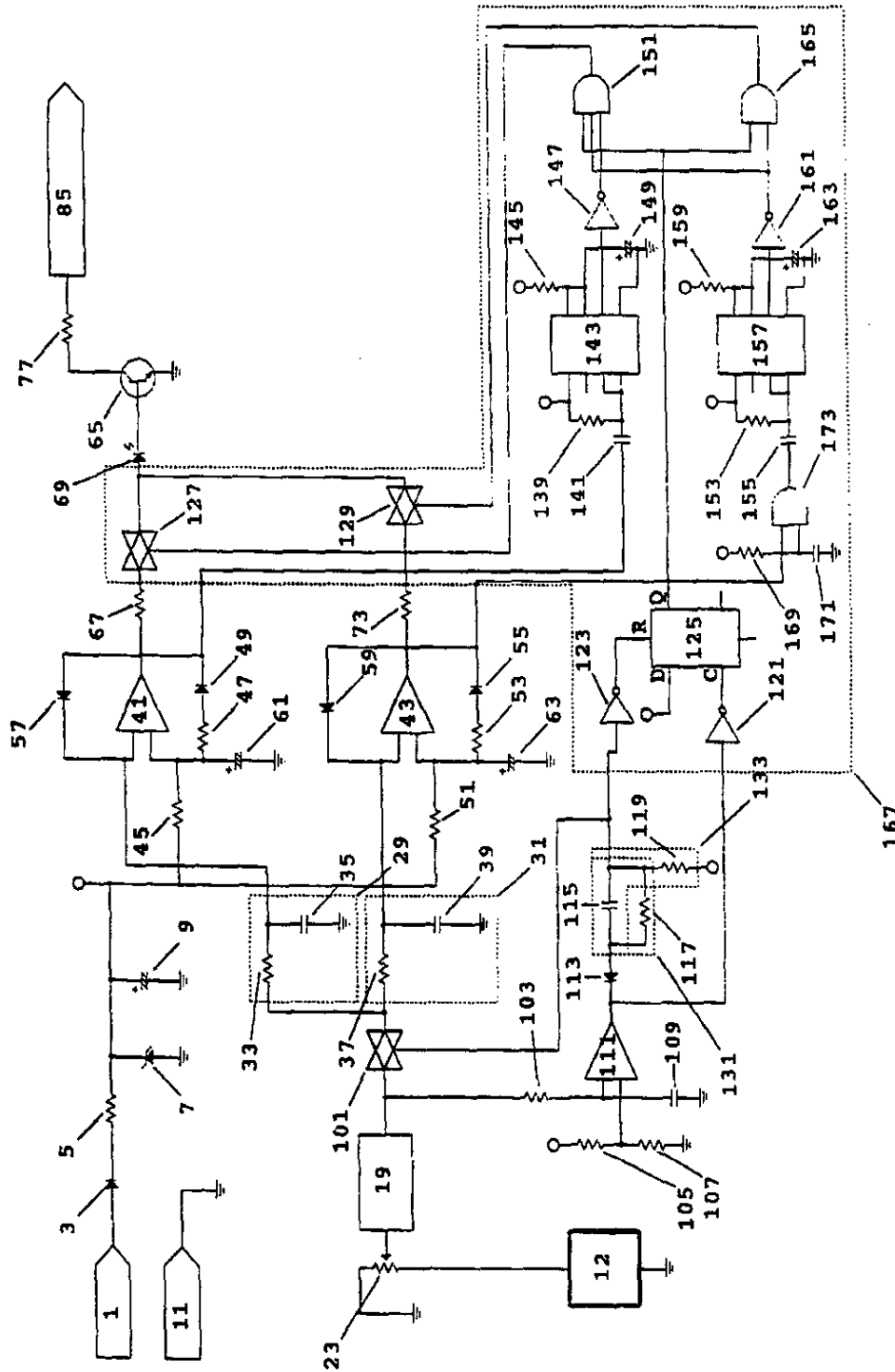


FIGURE 3

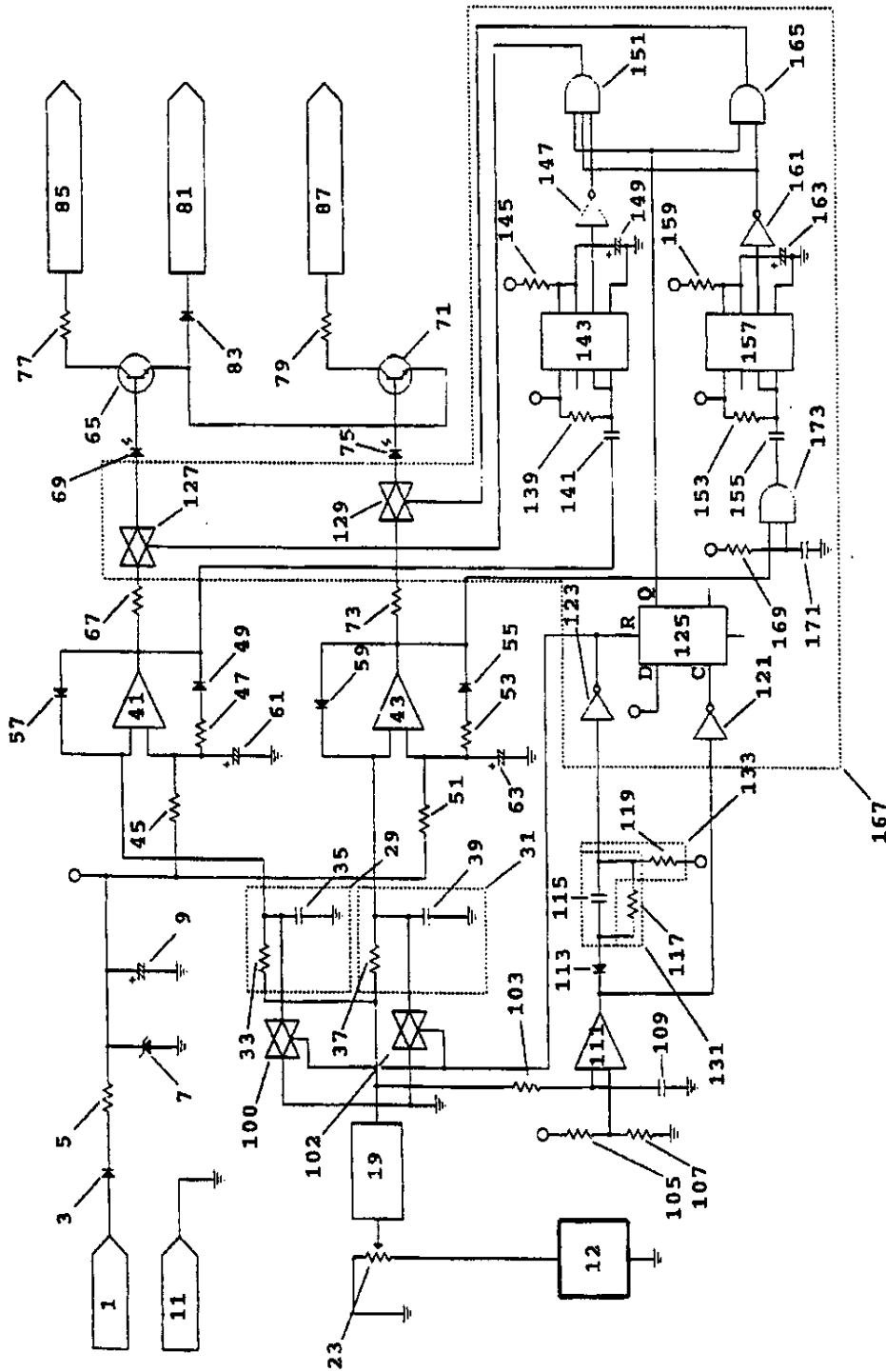


FIGURE 4

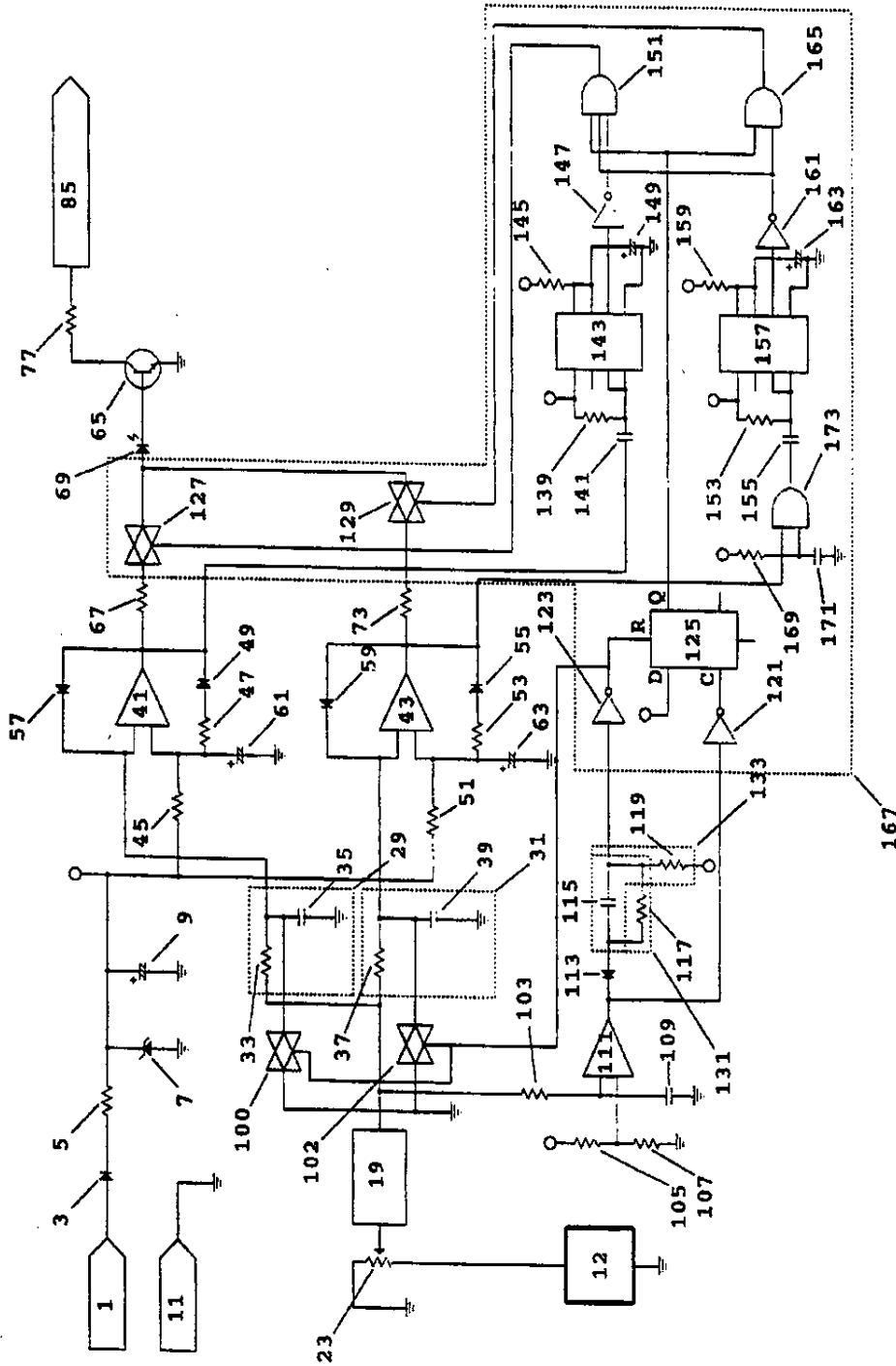


FIGURE 5

CMOS INTEGRATED CIRCUIT

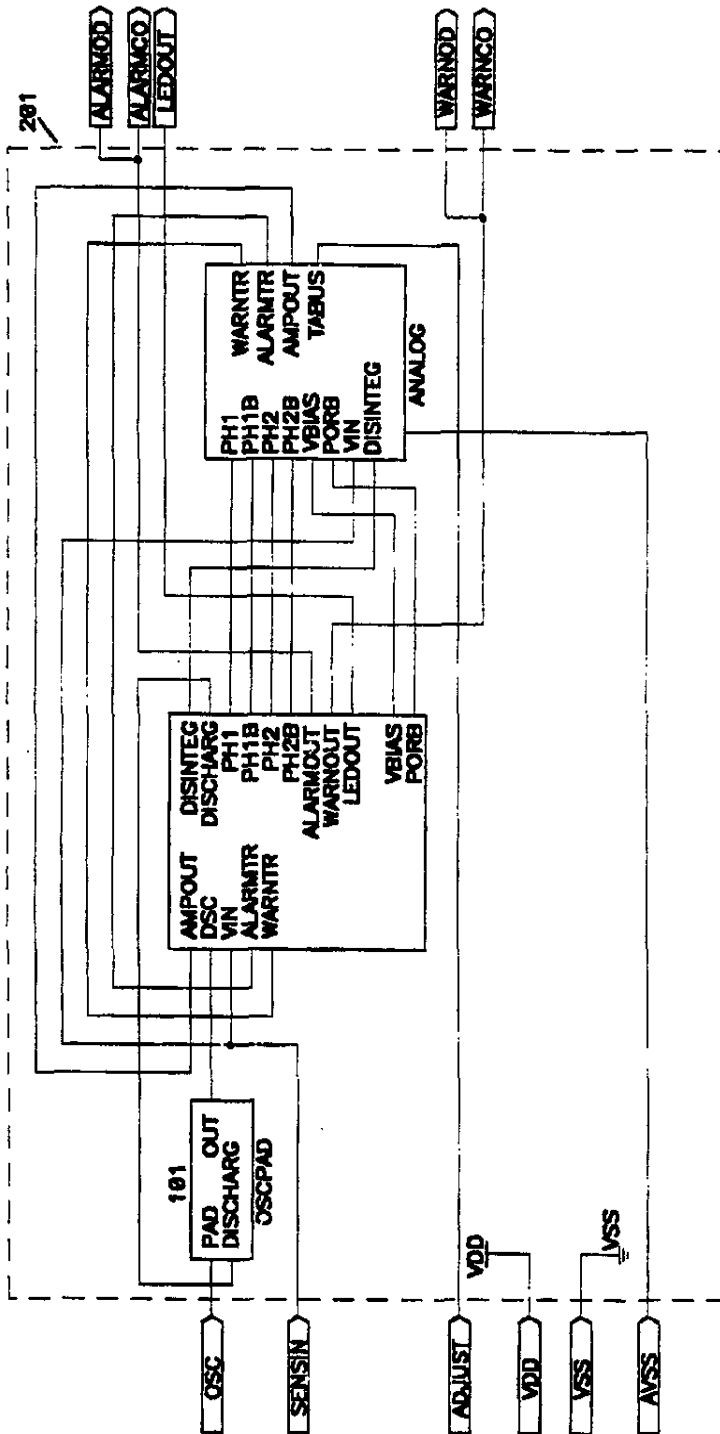


FIGURE 7

ANALOG SECTION

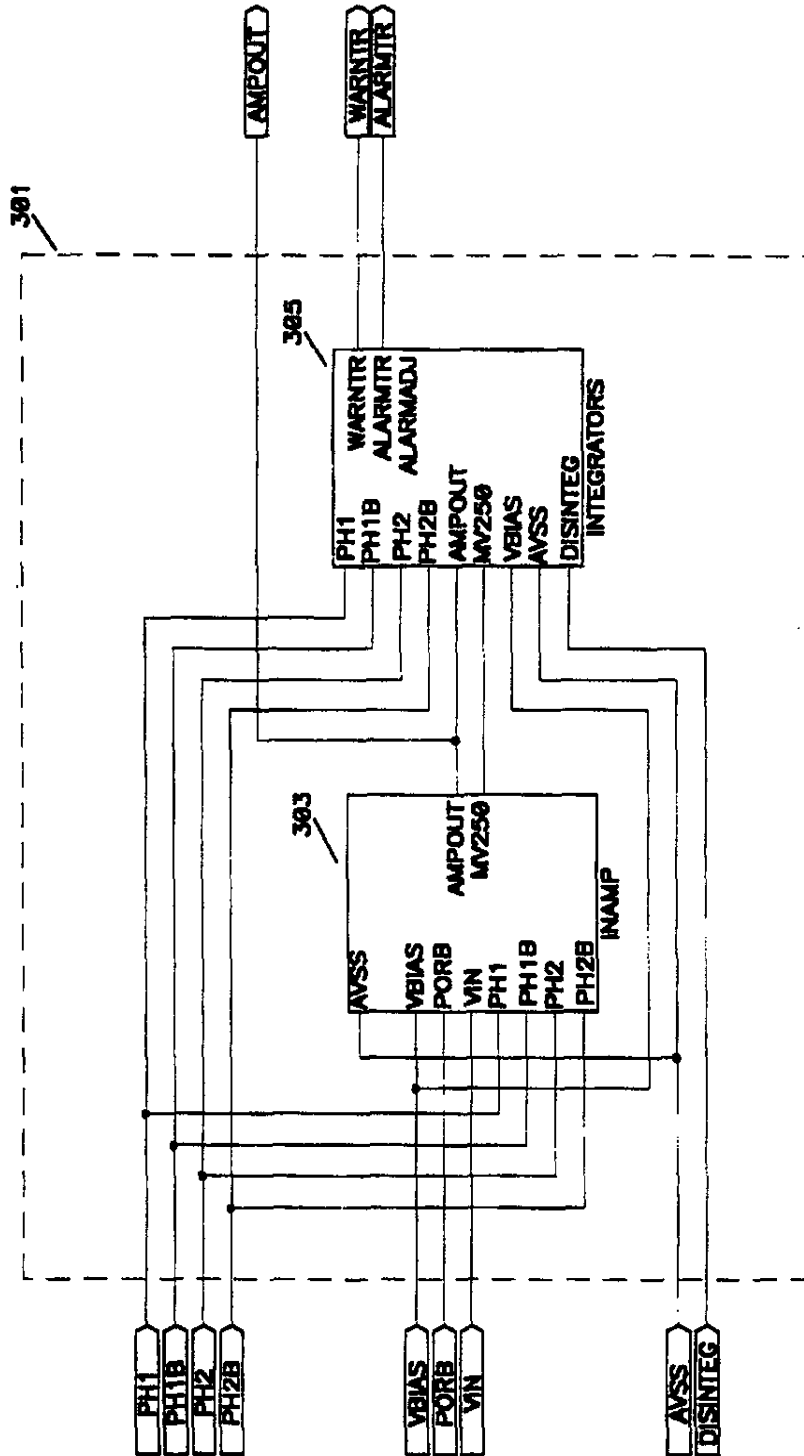


FIGURE 8

AV40AMP NEW

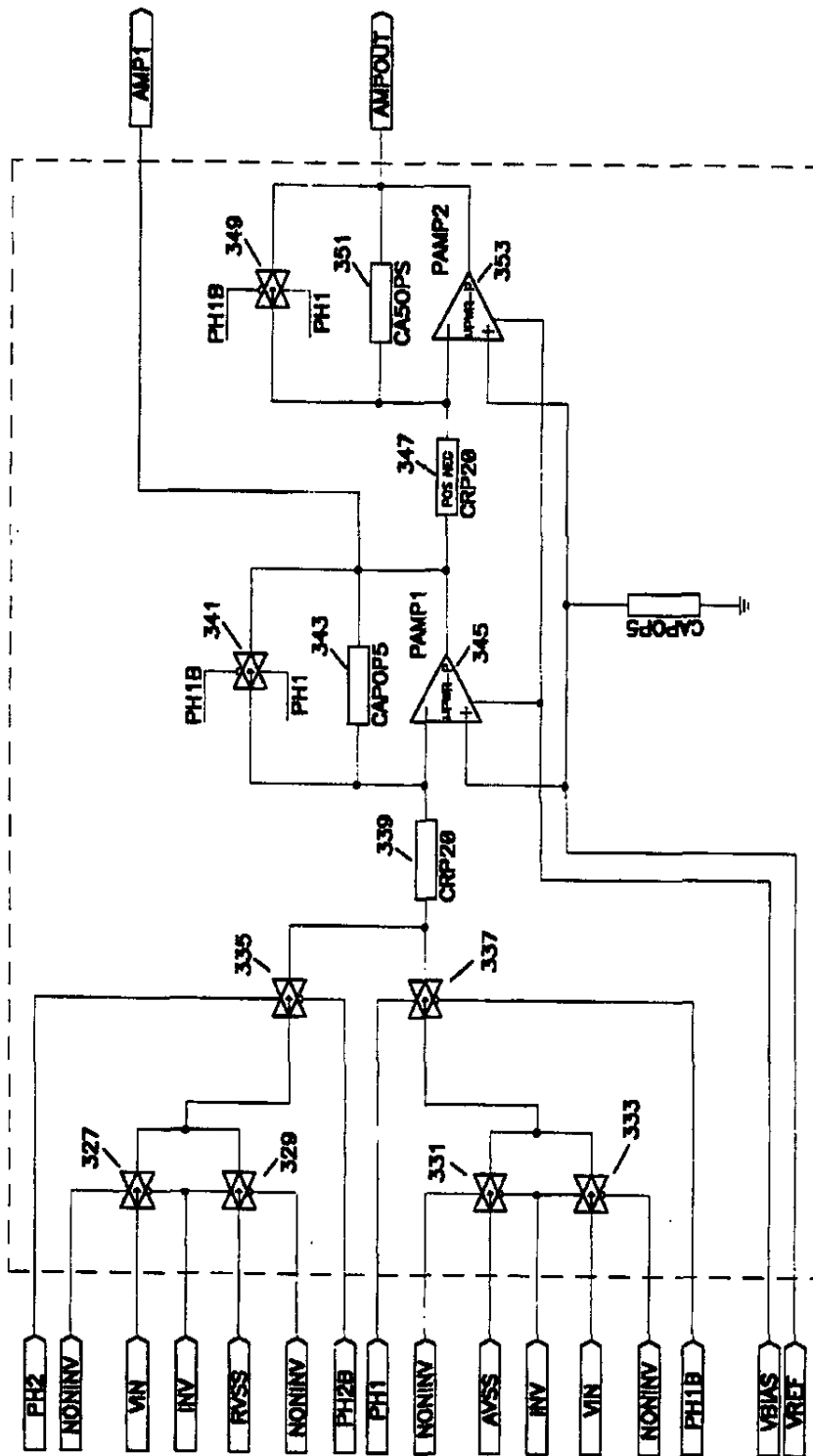


FIGURE 10

ALARM AND WARN INTEGRATORS

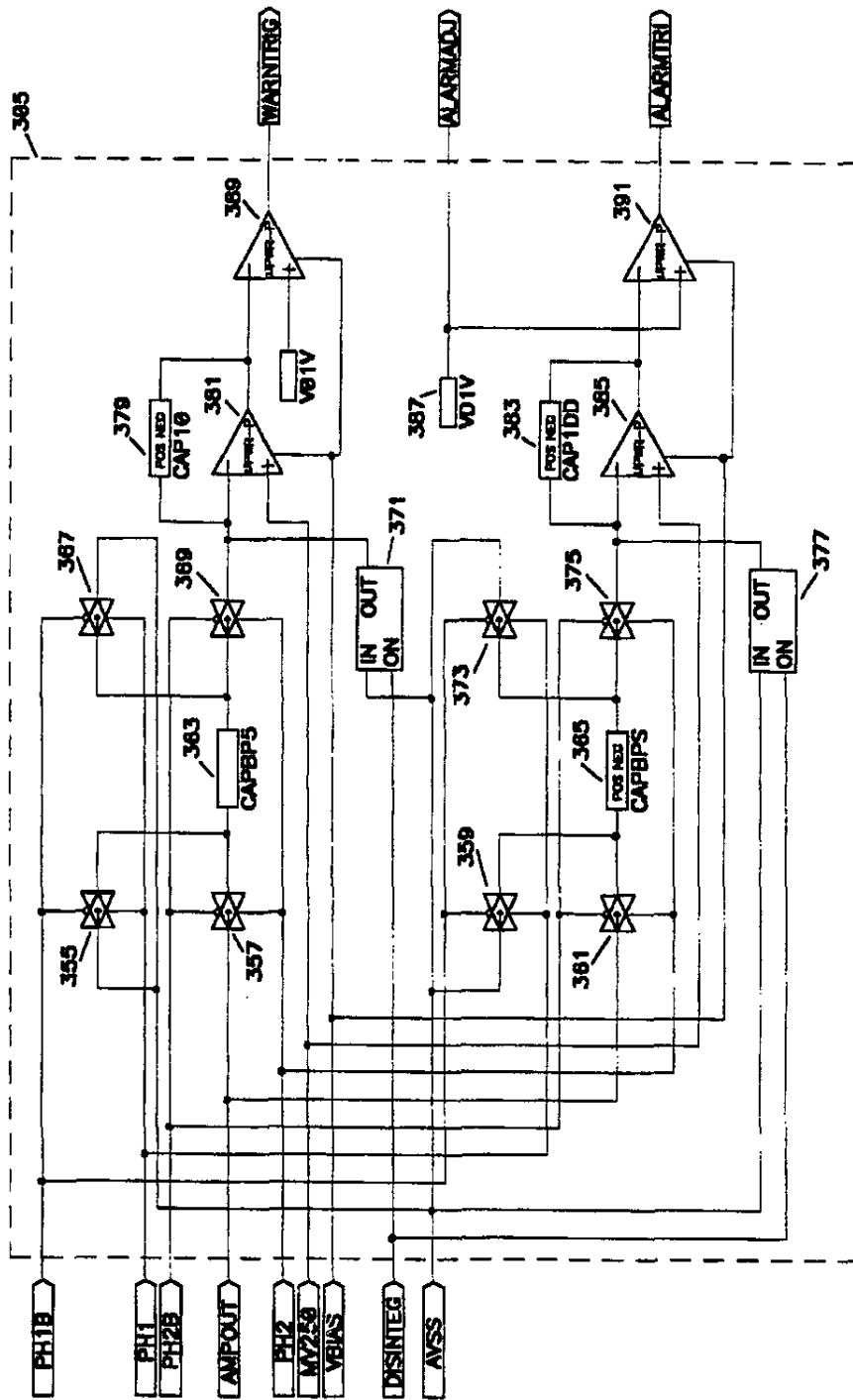


FIGURE 11

DIGITAL BLOCK

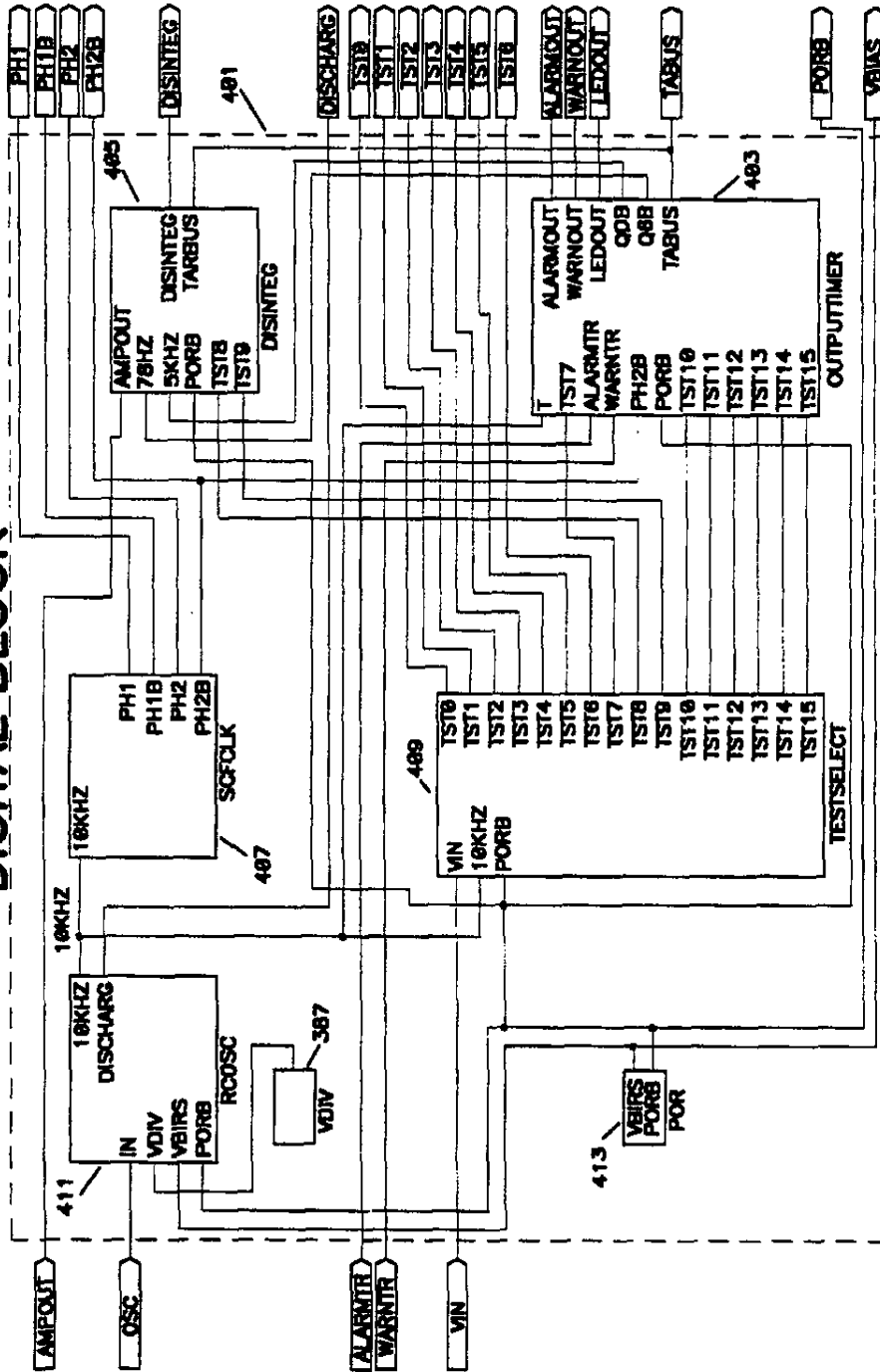


FIGURE 12

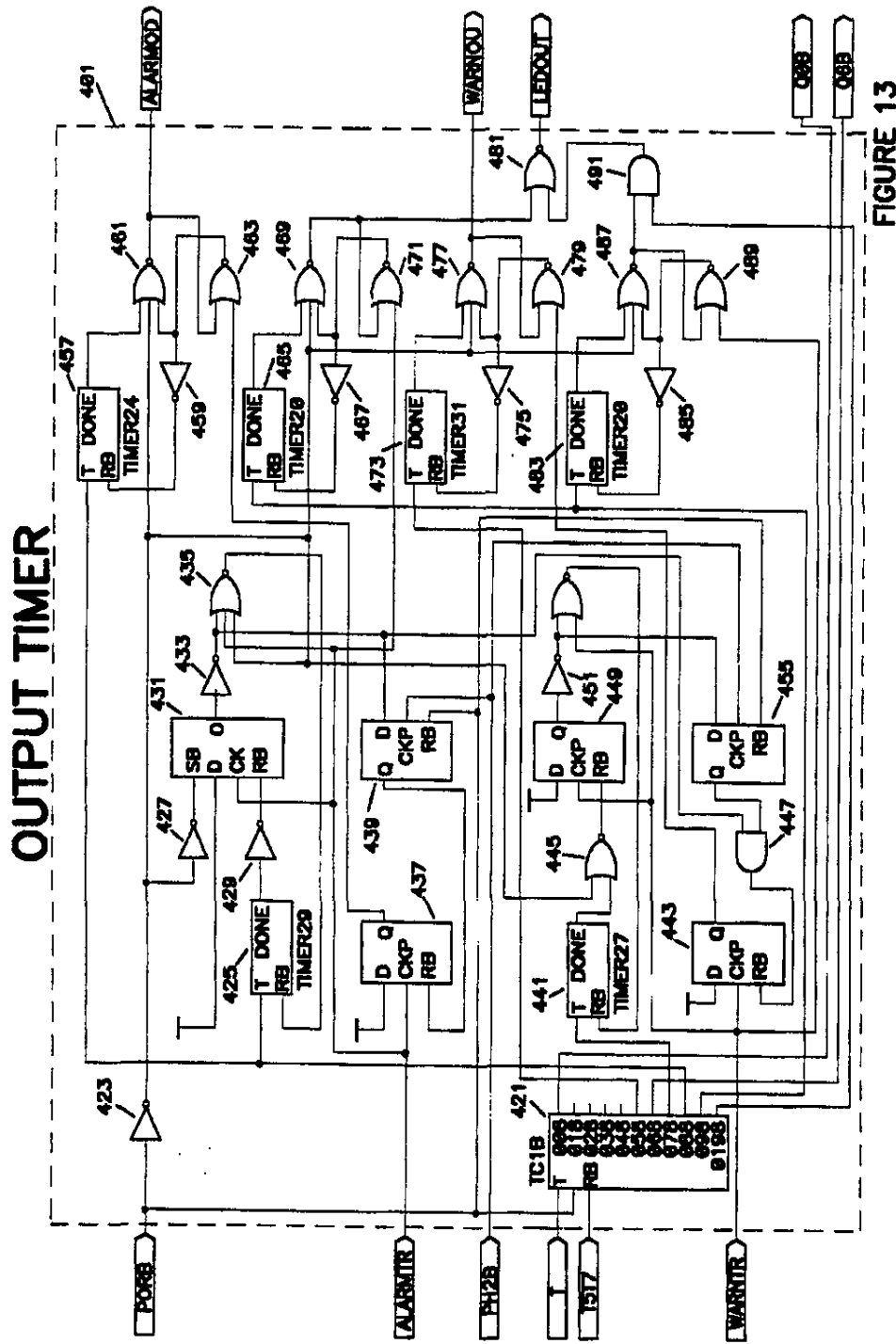


FIGURE 13

INTEGRATOR DISABLE

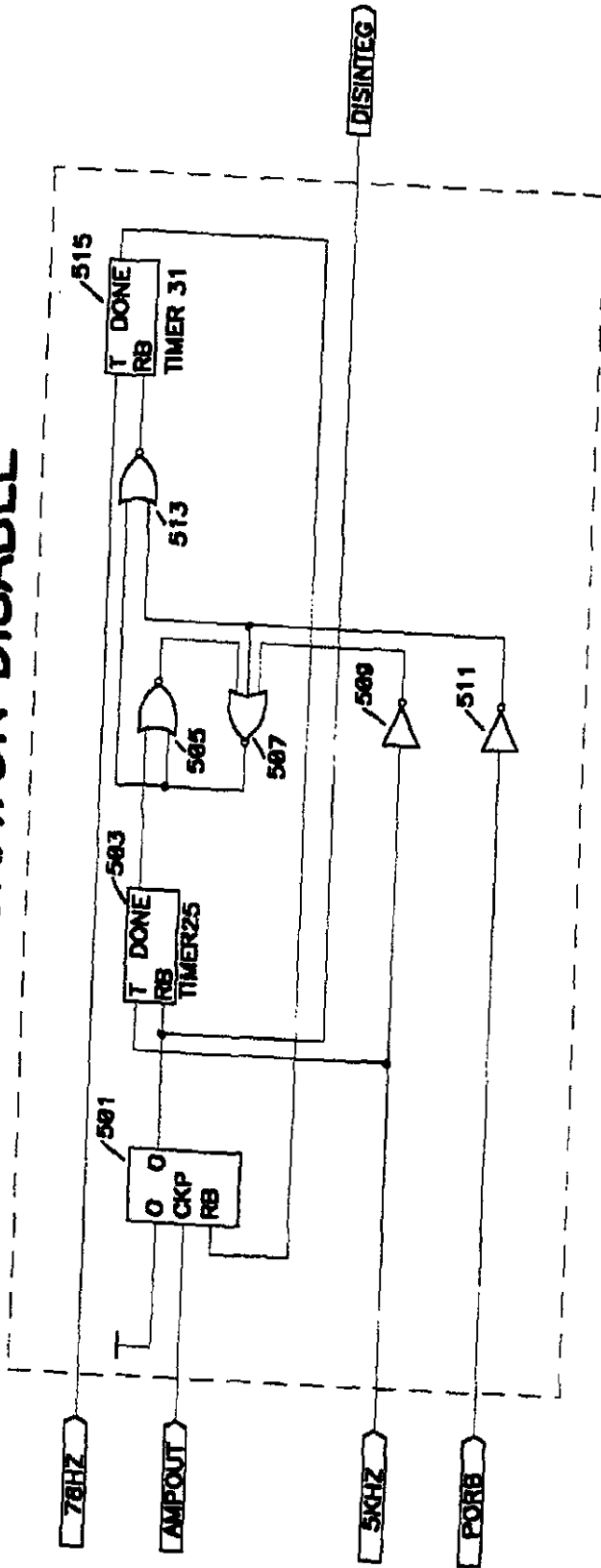


FIGURE 14

TIMER 31

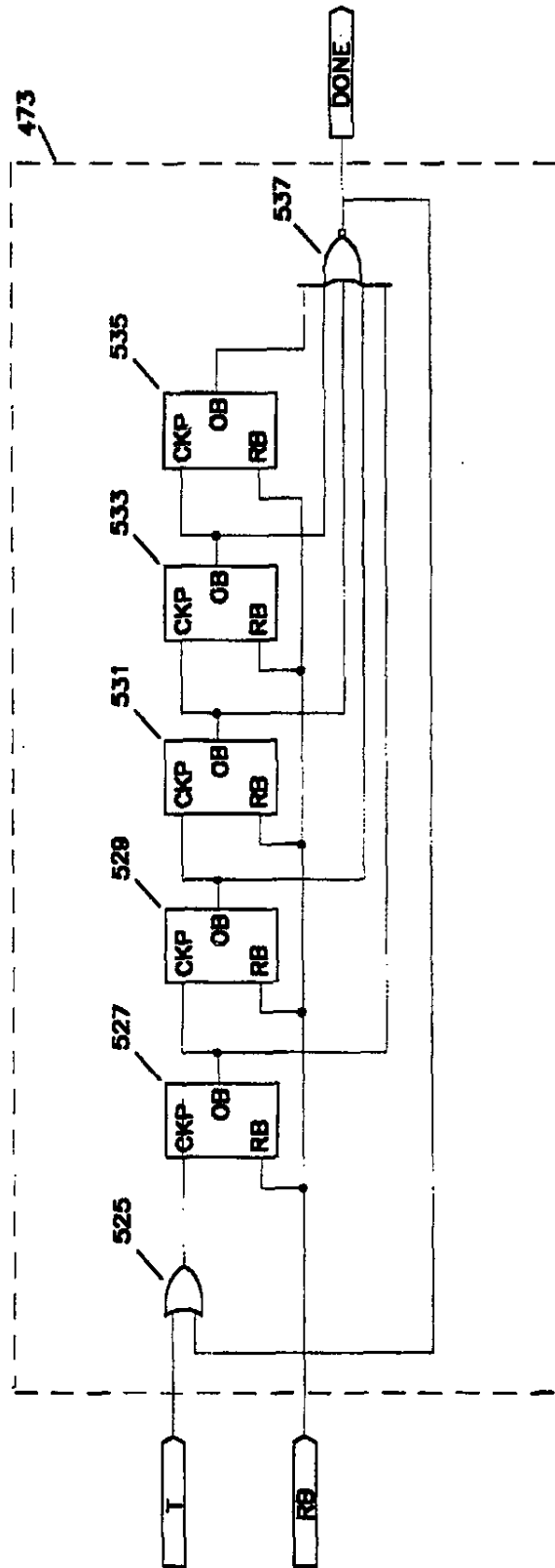


FIGURE 15

5,646,591

1

**ADVANCED METHOD OF INDICATING
INCOMING THREAT LEVEL TO AN
ELECTRONICALLY SECURED VEHICLE
AND APPARATUS THEREFOR**

**RELATION TO OTHER PATENT
APPLICATIONS**

This patent application is a continuation-in-part (C-I-P) of patent application Ser. No. 08/433,819 filed May 4, 1995, entitled "Method Of Indicating The Threat Level Of An Incoming Shock To An Electronically Secured Vehicle and Apparatus Therefor," now abandoned; which is a continuation-in-part (C-I-P) of patent application Ser. No. 08/112,940 filed Aug. 30, 1993, entitled "Method Of Indicating The Threat Level Of An Incoming Shock To An Electronically Secured Vehicle and Apparatus Therefor," now U.S. Pat. No. 5,532,670; which is a continuation-in-part (C-I-P) of patent application Ser. No. 07/886,871 filed May 22, 1992, entitled "Method Of Indicating The Threat Level Of An Incoming Shock To An Electronically Secured Vehicle and Apparatus Therefor," now abandoned. This patent application is also a continuation-in-part (C-I-P) of patent application Ser. No. 07/945,667 filed Sep. 16, 1992, entitled "Advanced Automotive Automation And Security System," now U.S. Pat. No. 5,534,845. Aforementioned U.S. Pat. Nos. 5,532,670 and 5,534,845 as well as applications Ser. Nos. 07/886,871 and 08/433,819 are hereby incorporated by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention pertains to the field of electronic security systems that detect unwanted intrusions into secured areas and sound an audible alarm in response thereto. More particularly, the invention pertains to a method of differentiating between a high degree of intrusion or threat such as a shock or a low intensity degree of intrusion or insubstantial threat, received by the protected structure or object, and executing an appropriate alarm as well as preventing nonphysical, random energy inputs from tripping the security alarm.

2. Description of the Prior Art

Electronic security systems have been used for some years and their popularity increases as the national crime rate continues to climb. Most such systems, especially those used for protection of automobiles, include a controller, a series of intrusion sensors for detecting attempted intrusions through doors, hood, and windows, an alarm for activation upon receipt of a signal or signals from the sensors indicating an attempted unwanted entry into the vehicle, and a power source, normally the vehicle battery, to power the system and sound the alarm. Other components are often included such as automatic resetting circuits and shut-down devices for use when the alarm needs to be deactivated. These systems may be original equipment on new vehicles or retrofitted on existing vehicles.

The security systems may be effected by a nonphysical signals, or electrical surges commonplace in the automobile circuitry. The intended arming and disarming of an alarm system is usually performed by sending a digitally coded signal, by a hand-held transmitter operated by one or more push buttons. In addition, other such systems may be armed by mere passage of time following the driver's act of turning off the engine and exiting the vehicle with the doors and windows closed and after a short time interval such as thirty (30) seconds. Thereafter the system may be disarmed by a

2

hand-held transmitter or by a delay circuit that activates the alarm if the system is not disarmed by the driver upon entry into the vehicle. The first type of arming is known as "active arming" while the latter is known as "passive arming".

Upon detection of an attempted intrusion into the vehicle by one of the sensors, the alarm is activated for a period of time, for instance thirty (30) seconds to one (1) minute, and then, if the alarm has not been disarmed by the remote transmitter or by the manipulation of a "kill" switch, mounted interior the vehicle, usually in a hidden area therein, the alarm response terminates or times-out and the security system is once again reset to monitor the sensors and triggers.

One form of such a sensor is called a "shock" sensor. The shock sensor technology of this invention is discussed in Applicant's patent application Ser. No. 08/112,940. However, a number of other sensors may be employed within the alarm system of this invention. This invention includes, but is not limited to, the application of shock sensors, motion sensors, field disturbance sensors, sound discriminators, ultrasonic sensors, current sensors and other sensors which sense disturbance or threat applied to or about an area and generate an electrical signal in response thereto. An incoming threat to the protected area such a vehicle includes threats such as physical impact, activity in or about the vehicle, breach of the vehicle electric system, the sound of breaking glass, or other activity results in the sensing of the activity and generation of an electrical signal which is then interpreted by the alarm controller to generate an alarm response.

Certain problems exist with conventional security systems that render their usage less than desirable under certain circumstances. For example, a shopping cart inadvertently bumped against the vehicle will usually cause a full alarm response. While the alarm is certainly necessary to alert the owner, inadvertent tripping of the alarm is annoying and could result in either the owner becoming frustrated, and thereafter not activating the alarm, or convincing the shopper or other car owners that such a loud, annoying alarm is not what they want in their vehicles.

In other situations, certain transient electric fields can invade the circuitry of the alarm system and generate enough of a signal to trip the alarm even in the absence of intrusion to the secured area. When a warn signal is generated by the alarm, it flashes the running lights which generates electrical surges or transients. These transients may generate electrical signals which may feed into the alarm circuitry where they are amplified and trip full alarm. In other situations, such as where a cellular telephone is used about the vehicle, the initial surge of the wireless transmission signal may be sufficient to generate an actuation level signal resulting in the activation of the alarm. Still further, in isolated cases, such as where a police car parks behind a protected area and the officer "keys" the microphone on his radio, the surge from his transmitter could interact with the anti-theft system induction coil and produce a false alarm.

Still further, there are instances where a disturbance continues unabated after the initial activation of the alarm sequence. For instance, a vehicle parked next to a train station may receive an alarm input generated by a passing train. The alarm will commence and terminate after running its course, yet often the train has not passed completely by the vehicle. In the prior art, the alarm will sound again because of the continuous input of energy from the train. This can be of annoyance to others in the area.

Crowded parking lots are prime areas for car theft. In these cases, dissatisfaction with the anti-theft system may

5,646,591

3

cause the owner to cease arming the system thus rendering the vehicle subject to theft. This condition, if not corrected, may cause other vehicle owners to cease purchasing such security systems for fear of annoying others and thereby undermine the desirability for and effectiveness of anti-theft devices.

What is needed to circumvent the drawbacks heretofore described is (1) a vehicle security system capable of differentiation between a light, generally non-threatening intrusion event and a stronger, usually security-threatening intrusion event to the vehicle and output a pulse to the alarm circuit appropriate to the degree of intrusion about the secured area, and (2) a vehicle security system that will discriminate between the non-threatening events and block them or otherwise divert the signals they produce so that an alarm is not generated.

SUMMARY OF THE INVENTION

This invention is a novel method of dealing with these problems and discriminating between the degree of threat from the incoming intrusion sensors. For example, the alarm system of this invention generates a mild audible chirp in the event one lightly touches a protected vehicle while loading groceries in a parking lot. Conversely, a full alarm response is generated if the car is towed or a crow-bar applied to its exterior. The low intensity alarm is called a "warn-away" and is of a serious, but far quieter nature and will generally generate the proper message of alarm presence to the intruder without engaging the full alarm. The person inducing the threat is thereby quietly, but convincingly advised by prerecorded voice or a series of soft chirps of the limited intrusion he or she has caused, without activation of ear piercing audible alarm response. Further, the owner and other people are not disturbed or embarrassed by a full alarm response caused by an innocent individual.

In addition, this invention includes the novel feature of providing full wave rectification of the output signal from the sensor and ignoring the first few milliseconds of the signal produced. Additionally, the present invention requires the signal to drop to its zero (0) level or reference voltage before triggering warning alarm. This allows an alarm condition to be registered only upon sensing actual intrusions on or about the protected area, as compared with non-physical intrusions generated by EMF or RF fields about the protected area. These features therefore eliminate the spurious signals that are produced by nonphysical threat conditions.

Most security systems involve only half-wave rectification of the induced signal emanating from the sensor. In the event the signal generated by a sensor generates a signal having positive and negative components the signal and in the event there is only partial rectification of the signal. The resulting rectified signal would be of unnaturally low value and not be an accurate reproduction or indication of the full intensity or degree of the incoming threat to the protected area. This practice is consistent with sensors employed to trigger the alarm system, but is unacceptable to the present invention which looks at the degree of the intrusion. Thus, to determine the degree of the intrusion sensed by a sensor, the present invention analyzes the peak to peak value of the sensor signals to determine the true degree of intrusion.

The method and apparatus disclosed herein analyzes the signal produced by various sensors having the capability of generating an electric signal upon sensing an intrusion event. Depending on the strength or value of the sensor signal, a mild or low intensity degree of intrusion generates

4

a pulse having a short pulse-width generating a warn-away alarm that will automatically reset itself without requiring intervention by the vehicle owner. The same method and apparatus is capable of generating a longer pulse-width pulse which generates both a mild, warn-away alarm response as well as a stronger, full alarm response.

When the low threat level, "warn-away" pulse is generated by the alarm system, the alarm system of this invention continues to monitor its sensors and is capable of immediate activation of a full alarm upon sensing a high degree of intrusion as reported by one or more of its sensors, even while a warn-away alarm is being given. If two or more mild shocks are received by the vehicle within a finite time period, seven (7) seconds for example, the system will produce a full alarm, whereas if the mild shocks are repeated on a sequence longer in time than seven (7) seconds, a second and repeated "warn-away" alarm will be produced again.

The prior art alarm system have not yet appreciated these features and continue to generate repeated "warn-away" or full alarms. In fact, in some cases the energy dispensed in the "warn-away" alarm is of sufficient magnitude to generate a low-threat level input that triggers another "warn-away" alarm so that the system continues to cycle "warn-away" alarms each induced by the preceding alarm.

Further, this invention contains the unique property of ignoring the first few milliseconds of signal produced by a sensor. A real threat condition usually lasts far longer than the ignored duration and the energy level of the residual signal is sufficient to pass through an integrator to a comparator to determine the relative degree of the threat. The signals produced by RF bursts, EMF bursts and other non-threatening or non-physical phenomenon typically do not last beyond that period and still cause a threat situation. Accordingly, those signals produced by non-physical and/or non-threatening phenomenon will be disregarded and will not cause the alarm systems to enter into an alarm condition.

To overcome the problem of repeated sirens during periods of extended sensor input, such as in the train passing example, or even when a truck or other heavy vehicle passes the parked car, means are provided to prevent repeated alarms as long as the initial input remains within a given intensity for an extended time. For instance, as long as the intensity level of the input signal remains rather constant following cessation of the full alarm signal, the circuit will not process another sensor input until this signal disappears and reappears again. This means that the prolonged motion the train passing nearby a protected vehicle, which generates a sensor input, will not cause the alarm to sound again and again. This feature also prevents continuous alarm outputs in those cases where the sensor is in a state of a continuous output. The state of continuous sensor output may be mechanical in nature (the train example) or from electrical disturbances.

In a second embodiment of this invention, the circuit is designed such that fewer wires need be used to attach the sensor to the alarm giving rise to a savings in material and reduction in installation time and training.

The prior art has recognized some of these problems, however, to date there has been little success achieved in solving them. In the patent to Hwang, (U.S. Pat. No. 5,084,967) a "motion detector" is allegedly connected to a pair of signal amplifier circuits that, upon receipt of a long signal or a series of short pulses from the detector, will sound a "full" alarm whereas, upon receipt of a shorter pulse signals, will sound a "pre-entry warning", lesser in severity

5,646,591

5

than the "full" alarm. However, this patent discloses that the "detector" is a time-dependent switch. Therefore the degree of threat is determined by its duration, not its physical degree. The schematic of the Hwang device shows the use of components that are arranged as a switch to turn on and off a transistor to allow the detected signal pass on to the alarm warning device. Thus, there is no comparison of the "level of intensity" of the signal, but merely the "duration" of the signal. This is not an accurate assessment of the degree of threat sensed by the sensor and reproduced into an electrical signal and does not differentiate between "intensities" of the physical and non-physical inputs. Moreover, the output signal from the device of Hwang Patent proceeds directly to the siren, whereas the device of the present invention interposes another device, the alarm control module or alarm controller, that determines what level of alarm is generated.

Accordingly, the main object of this invention is a method and apparatus for use on about an electronically secured area that responds differently to different degrees of threat sensed by the sensors arranged therein. Other objects of the invention include a method and apparatus that has at least two levels of intensity determination, one for a low degree of threat received by the vehicle to produce a pulse that may be used to trigger a warning of a stronger alarm, should the threat not be discontinued, and a separate pulse that may be used to trigger a stronger, louder alarm for non-discontinued light shocks and stronger shocks; a method and apparatus for producing a pulse that may be used to trigger a warn-away audible alarm that may be repeatedly sounded to signify the vehicle is under electronic security while not producing a pulse that may trigger the loudest alarm so as to minimize the disturbance to those nearby in the event of a non-threatening disturbance received by the vehicle; a method and apparatus that maintains readiness to produce a pulse that may be used to trigger an audible alarm even while a warn-away alarm message is being used; a method and apparatus for detecting a signal produced by a non-physical assault on the vehicle, such as by a burst of RF energy or EMF energy, and for removing it from interaction in the system circuitry; a method and apparatus that provides full wave rectification of the induced signal to provide a more accurate analysis of the threat inducing the sensor signal; an apparatus which does not continue to sound an alarm in the event a generally constant and continuous disturbance such as a moving train; an apparatus having the ability to communicate the level of threat in a pulsewidth of the sensor output pulse, thereby eliminating a dedicated wire connection for each alarm stage; an apparatus that may be retrofitted into existing vehicles as well as included as original equipment on new vehicles; and, an apparatus that will automatically rearm upon the completion of a measured length of the warn-away or the full alarm; circuitry that can be maintained in an integrated circuit thereby providing economy of manufacture, improved reliability, space savings and less power consumption. These and other objects of the invention may be obtained by reading the following specification along with the drawings that are appended hereto. The protection sought by the inventor may be gleaned from a fair reading of the claims that conclude this specification.

DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic diagram of the apparatus of this invention;

FIG. 2 is a flow diagram illustrating the operation of the apparatus generally depicted in FIG. 1;

6

FIG. 3 is a schematic diagram of an alternate embodiment of the apparatus, showing less wiring needed to accomplish the same functions as shown in FIG. 1;

FIG. 4 is a schematic diagram of an alternate embodiment of the bilateral switch wiring shown in FIG. 1;

FIG. 5 is a schematic diagram of an alternate embodiment of the bilateral switch wiring shown in FIG. 3;

FIG. 6 is a top level schematic representation of an alternate embodiment of this invention;

FIG. 7 is a top level block diagram of CMOS Integrated Circuit and its analog and digital sections;

FIG. 8 is an intermediate level block diagram of the analog section, showing the amplifier block and the integrator block;

FIG. 9 is a schematic/block diagram of the amplifier block and its inverting/noninverting determination circuitry;

FIG. 10 is a schematic diagram of the amplifier block;

FIG. 11 is a schematic diagram of the warnaway alarm and full alarm switching capacitor integrators and their associated circuitry;

FIG. 12 is an intermediate level block diagram of digital section, showing its major blocks therein;

FIG. 13 is a schematic of output timer block having six timer blocks, timer clock divider block and the associated circuitry required to support the timing of the IC;

FIG. 14 is a schematic of the integrator disable control circuit; and,

FIG. 15 is a schematic of one of the five stage "T-flip-flop" timers that is used in IC.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The novel method of this invention for indicating the threat level of an incoming threat to an electronically secured structure, such as a vehicle comprises, the steps of sensing a threat delivered to an area, generating an electric signal the strength of which is proportional to the intensity of the threat, ignoring the first portion of the signal so as to remove from further consideration those disturbances that are non-physical or non-threatening, analyzing the remaining signal to determine if it is of a low, generally non-threatening intensity or of a higher, generally security-threatening intensity, and producing either a first pulse that triggers a low intensity "warn-away" alarm, or separate first and second pulses, representing a signal containing both the low intensity and higher intensity components, that trigger both a low and a high intensity alarms. The step of generating an electric signal includes generating an alternating current signal whose amplitude and period is proportional to the intensity of the physical shock. FIG. 1 shows the apparatus of this invention.

In FIG. 1 the solid lines between components refer to conductors and will not be individually numbered except where necessary. Where conductors cross and the intersection is marked with a dot or period, it is a junction; where one conductor crosses another and the intersection has no dot or period, there is no junction. As shown in FIG. 1, an input voltage, generally in the range of from about six to about eighteen volts d.c. is inputted from a battery (not shown), such as a car battery or other source of direct current, to an input terminal 1. The current is regulated by a reverse flow protection diode 3, a surge limiting resistor 5, an over-voltage protection Zener diode 7 and a filter capacitor 9 to produce a steady flow of direct current. The ground return enters at input terminal 11.

5,646,591

7

The sensors employed by the present invention are interchangeable. Different sensors are employed for different functions within the alarm system and their selection depends in large by the anticipated environment within which the user expects to keep the protected property. Some of the more common sensors are shock sensors, motion sensors, field disturbance sensors, sound discriminators, ultrasonic sensors and current sensors. The shock sensors known in the art are mechanical, mercury movement, magnetic induction, and piezo types. Applicant's patent application Ser. No. 08/112,940 disclosed Applicant's preferred embodiment of the shock sensor.

Mechanical shock sensors use a weighted cone at the end of a spring which makes electrical contact with a fixed pointer upon an impact, creating an output pulse.

Mercury sensors consist of two designs. The first design is the mechanical contact type. The second design is one in which mercury is suspended inside an inductor that is part of an electronically tuned circuit. In both designs an impact results in the mercury remaining in a fixed position, while everything else moves about with the impacted vehicle.

The magnetic induction shock sensor uses a magnet suspended by an elastic band such as rubber, silicon or spring near a high value inductor. The inductor usually has an iron or ferrite core. An impact moves the sensing inductor while the magnet remains fixed, creating an impact AC signal in the inductor. The signal is typically amplified, detected, integrated and then compared with preset levels to determine whether or not to generate an output signal.

The piezo shock sensor uses a weighted piezo sensor. A mechanical resonance of approximately seventy (70) hertz is created by adding mass to the piezo sensor. This aids in the detection of impacts to the vehicle. Similarly, the weight remains fixed while the balance of the piezo sensor moves about with the impact to the vehicle.

Another type of sensor employable by this invention is a motion sensor. Motion sensors sense very slow movements of the vehicle. These movements could be caused by jacking, lifting, moving, or any other type of slow movement of the protected object. These movements may be sensed by several methods such as a weighted pendulum with mechanical or electronic contact, mercury movement switch or mechanical/electronic movement sensing devices, or any other slow movement sensing system.

Another type of sensor employable by this invention includes a field disturbance sensor. Field disturbance sensors sense motion of objects such as the human body in a microwave radio frequency field in or about the protected area. The presence of the moving object disturbs the microwave field and creates a disturbance therein. This results in a change of the sensor output signal. This disturbance is both reflective and absorptive in that all objects absorb and reflect RF energy. A multichannel sensor generates an output signal proportional to intensity of the detected disturbance. A single channel sensor only generates a signal if the present threshold is exceeded. Additionally, a pulsed microwave signal could be generated to look for time of signal return. This, however, requires a more complex sensor and circuit than the above field disturbance sensor.

Another type of sensor employable by this invention includes a sound discriminator. Sound discriminator senses a high frequency sound disturbance in or near the protected area and is normally used to sense the breaking of glass and/or metal to metal sounds. The sensor normally uses an electric condenser microphone to sense the sound and convert it to an AC signal. This AC signal is amplified and

8

processed through a high pass and/or band pass filter(s). The signal is then detected and compared to preset thresholds. An output pulse indicative of the intensity of the disturbance is then generated and output.

Another type of sensor employable by this invention includes an ultrasonic sensor. An ultrasonic sensor can work on the same principle as the field disturbance sensor (doppler frequency shift), but uses an ultrasonic sound field instead of an RF energy field. In a second embodiment, the sensor uses an ultrasonic sound generator (transmitter) to set up a field of sound waves usually at forty (40) kilohertz. An ultrasonic sensor (receiver) then detects any disturbance. This signal is then amplified and detected generating an output pulse or pulses according to the level of disturbance. In a third embodiment, the ultrasonic sound could be pulsed to measure the movement of and distance to the object creating a disturbance.

Another type of sensor employable by this invention includes a current sensor. Current sensors sense the change in battery voltage caused by the activation of devices which in turn produces a current load. There are at least two different types of current sensors. One type senses only small changes in voltage created by any load being turned on, while the second type detects a sudden large change in voltage, such as a surge created by incandescent lights being turned on. The first type of sensor is simpler and easier to manufacture, while the incandescent light sensor does not require an external input to disable the circuit when the vehicle automatic electrical cooling fans turn on. The current sensor is usually employed to sense the under hood, trunk, and/or dome lights turning on when an unauthorized entry is made.

Each and every sensor heretofore mentioned senses a particular type of intrusion and produces an electrical signal proportional to the degree of threat sensed. Other types and kinds of sensors capable of sensing particular conditions and providing an electrical signal in response thereto are not mentioned, but are contemplated within the scope of this invention. The above mentioned sensors will be collectively referred to as sensor means 12.

The step of analyzing the signal to determine if it is of a low or high intensity includes the first step of passing the signal through a switching capacitor amplifier 19 to provide full wave rectification, i.e., the negative portions of the signal are converted to positive portions. Accordingly, the output of amplifier 19 is always positive and will give an approximately equal output regardless of the polarity of sensor means 12 signal. This overcomes the shortcomings of a sensor having a signal operating in the positive and negative region in respect to the system ground. This allows the entire dynamic range of the signal to be offset/rectified to a positive voltage. The gain of amplifier 19 is fixed at a predetermined value. A potentiometer 23 is used to adjust the level of the input from sensor means 12.

A normally closed, analog, bilateral switch 101 is provided and connected between amplifier 19 and an inverting comparator 111. In other embodiments of the invention comparator 111 is not inverting. It is opened for a predetermined amount of time such as a few, i.e., 5, milliseconds at the beginning of each pulse string, as will be hereinafter more fully set forth, in order to cut off, delete or disregard the first portion of the signal output from amplifier 19. This cut off is employed to prevent extraneous, non-physical energy surges, such as RF and/or EMF fields, as hereinbefore described, from tripping the alarm.

Another significant feature of the present invention provides for removal from consideration of signals which do

5,646,591

9

not disappear and later reappear. The signals which do not disappear and later reappear are disregarded by this device to prevent continuous alarm outputs which are a nuisance. This is particularly helpful where the alarm system is operating in an area having exposure to phenomenon of prolonged duration such as a freight train passing nearby the alarm system. As the train passes, it generates a vibration which likely has an intensity sufficient to generate an alarm. In practice, this type of disturbance is not well received by alarm systems because the alarm system will generate an alarm which ceases after a predetermined time and which is regenerated again and again as long as the disturbance continues about the area. This provides for much frustration to the owner of the alarm system and the people nearby, thereby reducing its effectiveness. To overcome this problem, the alarm of the present invention monitors the signal causing the alarm. In the event this signal/disturbance continues to be present at a generally constant intensity for a time greater than the duration of the alarm response, the second and subsequent alarm responses are not generated until such time as the signal generated by the disturbance disappears and then reappears again. In practice this provides for one cycle of alarm response if the alarm system detects a disturbance such as a moving train. The alarm response will not be repeated over and over again until such time as the disturbance caused by the train disappears and then later reappears.

Switch 101 is nominally in a closed position and is held closed by the power supply voltage less voltage drop through resistor 119. Shutting off or opening of switch 101 is accomplished by use of an inverting comparator 111 and its associated circuitry. Resistors 105 and 107 establish a reference voltage for comparator 111. Resistor 103 and capacitor 109 filter out high frequency transients on the input to comparator 111. In the event a continuous high frequency signal is present at the input of sensor means 12 or at the output of amplifier 19, the high frequency filter 103 and 109 could lead to a continuous, low DC signal output at the output of comparator 111. This inhibits clocking of D flip-flop 125 which in turn opens switches 127 and 129 until the output of comparator 111 changes state and produces a clock signal at the clock input of D flip-flop 125.

As a signal inputted to comparator 111 goes high, the output of comparator 111 goes low and is coupled through a diode 113 and a capacitor 115 to switch 101. Therefore the source voltage for keeping switch 101 in its closed position is shorted for a predetermined duration of time through capacitor 115, which provides for opening of switch 101 for that duration of time. By adjusting the capacitance of capacitor 115, a delay, such as 5 milliseconds is required to charge capacitor 115 in order to turn bilateral switch 101 back on. Resistor 117 is provided as the discharge resistor for capacitor 115 and its value is chosen so that capacitor 115 will not discharge for several hundred milliseconds so as not to interrupt the signal pulse string. The discharge time of capacitor 115 is such that only the first few milliseconds of any pulse string is allowed to be coupled through capacitor 115 and diode 113 to shut off analog bilateral switch 101.

The next step, after passing the amplified signal through switch 101 is to input this amplified signal simultaneously to two separate and independent voltage integrators, 29 and 31, shown within dotted line perimeters, that are connected in parallel to the output of amplifier 19. Integrator 29 comprises a resistor 33 and a capacitor 35 while integrator 31 comprises a resistor 37 and a capacitor 39. The ratio of sensitivity of integrators 29 and 31 is adjusted, by varying the resistance of resistors 33 and 37 and varying the capaci-

10

ance of capacitors 35 and 39 to the order of approximately 5:1 so that integrator 29 is approximately five times as sensitive as integrator 31. This ratio can be varied outside of 5:1 under certain circumstances such as where the vehicle is unusually large.

The next step is to send the output of integrators 29 and 31 to a pair of separate voltage comparators/pulse generators 41 and 43 that are equally referenced from input terminal 1. The reference for voltage comparator 41 is established by resistors 45 and 47 and a diode 49 while the reference for voltage comparator 43 is established by resistors 51 and 53 and a diode 55. Another pair of diodes 57 and 59 are used to latch the respective voltage comparators 41 and 43 when their respective input signals exceed the comparator reference voltages.

The next step in this novel method is for the pulse generator portion of comparators/generators 41 and 43 to output either a first pulse from generator 41 representing a low intensity signal or separate first and second pulses from both generators 41 and 43 representing a signal containing a low intensity and a high intensity component. This is performed when voltage comparator 41 or 43 is latched through either diode 57 or diode 59 when the incoming signal from integrators 29 or 31 exceeds the reference voltage thereto. Once latched, the respective comparator produces an output pulse timed by resistor 45 and capacitor 61 with respect to comparator/pulse generator 41 or by resistor 51 and a capacitor 63 with respect to comparator/pulse generator 43 to one of two drive transistors 65 and 71.

Output drive transistor 65 receives the output pulse from voltage comparator/pulse generator 41 through a resistor 67 and an indicating light emitting diode 69 for the duration of the pulse from generator 41. The other output drive transistor 71 receives the output pulse from voltage comparator/pulse generator 43 through a resistor 73 and an indicating light emitting diode 75 for the duration of the pulse from generator 43. Resistors 77 and 79 are current limiting resistors employed to protect transistors 65 and 71 respectively. The outputs are enabled by a ground placed on terminal 81 through a diode 83. The outputs are fed respectively to terminal 85 to connect to a warn-away alarm circuit (not shown), and to terminal 87, to connect to the full alert alarm circuit (not shown). The output pulse for the warn-away alarm, from terminal 85, may be set at one length, such as 200 milliseconds, and the output pulse for the full alarm from terminal 87 may be set at a different length, such as approximately 1 full second.

The negative voltage, 5 millisecond pulse from comparator 111 is inverted by inverter 123. This provides a logic one pulse which resets and holds in reset for the 5 millisecond period (determined by capacitor 115) the "D flip-flop" 125. This achieves the function of discarding from consideration a continuous signal having a frequency such that this signal represents a DC signal at input of comparator 111. Thus, this signal will eliminate any clock activity to D flip-flop 125 until such signal disappears and again reappears. The "Q" output of 125 is connected to the inputs of "AND GATES" 151 and 165, causes the outputs of 151 and 165 to go low. The low signals at the outputs of 151 and 165 opens normally closed analog bilateral switches 127 and 129. This prevents any output from pulse generators 41 and 43 being coupled to output transistors 65 and 71.

After the end of the 5 millisecond reset pulse, the "Q" output at flip-flop 125 is set high by a clock signal created by comparator 111. This clock pulse is inverted by inverter 121 to present the proper input to the 125 clock input. The

5,646,591

11

sensor outputs 85 and 87 are now enabled for the duration of the output pulse(s) created by pulse generators 41 and 43.

As mentioned before, this invention provides for the embodiment where the alarm will not be continuously triggered by a relatively constant threat signal which persists without interruption. One application for this feature is an armed alarm system which is triggered by a train. Ordinary alarm systems continue to sound its warning for the duration of the threat signal. The alarm system of the present invention provides for a single cycle of alarm and does not sound the alarm again until the threat signal disappears and again reappears. Therefore in the example of the passing train, the alarm would sound for one cycle, such as 2.5 seconds for the warn-away and 30 seconds or a minute for a full alarm, and as long as the train threat does not disappear (i.e. the train passed) and again reappear (i.e. another train appears) the system of the present invention will not sound the alarm again. The following circuit provides this function.

Output bypass timers 143 and 157 are triggered and reset from the trailing edge (negative going edge) of the output pulses from 41 and 43 respectively. The output of full alarm pulse generator 43 is applied to timer 157 via AND gate 173. When any input of an AND gate goes low, its output goes low. All inputs of an AND gate must be high to get a high at its output. These triggers are coupled to the inputs of the 555/556 timers by coupling capacitors 141 and 155 respectively. Resistors 139 and 153 are pull-up resistors on the trigger input of their respective timers. Resistor 145 and capacitor 149 control the time that the "warn-away" output is disabled. Resistor 159 and capacitor 163 control the time that the "alarm" output is disabled. When the timers are triggered/reset, the timing capacitors 149 and 163 are discharged, the outputs go high, and the timing cycle is started. The outputs will go low at the end of the timing cycle.

The high output from warn-away bypass timer 143 is inverted by inverter 147 and applied to AND gate 151. The low at the input of 151 causes the output of 151 to go low opening bilateral switch 127. This interrupts any output from 41 and disables the warn-away output drive to output transistor 65. All warn-away outputs are therefore disabled anytime that warn-away bypass timer 143 is running. All repetitive triggers that occur inside the timing window are bypassed (disabled) on the warn-away output until the warn-away bypass timer expires (approximately 1/2 second). While the timer is running, if the output at 41 goes low (output pulse expires), the timing capacitor is discharged, and the timer is restarted with a full charging cycle duration to run.

Full alarm bypass timer 157, upon receiving a negative pulse from the trailing edge of the output pulse from 43 via AND gate 173, works identical to the warn-away bypass timer 143. The high output from 157 is inverted by inverter 161 and applied to AND gates 151 and 165. The low at the inputs of 151 and 165 causes the outputs of 151 and 165 to go low. This low output in turn is applied to the control input of bilateral switches 127 and 129. Both output drives are interrupted, disabling both outputs (warn-away and full alarm) for the duration of the full alarm output bypass timer 157 (several seconds).

The full alarm bypass timer 157 is also used as a power up reset timer. At power on capacitor 171 is fully discharged, applying a low at the input of AND gate 173. Capacitor 171 is slowly charged bias resistor 169 removing the low input from AND gate 173. The output of 173 is low during this charging period triggering full alarm bypass timer 157.

12

Therefore, at power up, both outputs are disabled for several seconds until timer 157 times out.

FIG. 2 shows the flow of the induced signal and produced pulse through the circuit of FIG. 1. The sensor of sensor means 12 generates a signal the strength of which is proportional to the intensity or degree of the threat. Amplifier 19 provides full wave rectification and amplification of the signal for presentment through switch 101 to integrators 29 and 31 in parallel for integration of the total value of the pulse train less the first part thereof cut off by switch 101. The respective sensitivities of integrators 29 and 31 help to differentiate between a lower degree of threat which is likely non-threatening in nature and a higher degree of threat that represents a potential intrusion into the vehicle. The separate voltage comparators/output pulse generators 41 and 43 complete the differentiation and output a pulse to the output indicator and driver that results in one or both alarms being activated.

Amplifier 19, referenced by voltage from the car battery, amplifies all signals received from the sensor means 12. Integrators 29 and 31 ignore any signal whose peak-to-peak voltage is equal to or less than the amplifier reference voltage. Hence, very low signals generated by the sensor means 12 will not produce a signal or signals sufficient to activate voltage comparators/output pulse generators 41 and 43 to latch the respective unit and produce a pulse to be sent on to output drive transistors 65 and 71.

Upon receipt of a low degree threat signal, above the reference level of amplifier 19, the circuit will operate to activate voltage comparator 41, latch it, and produce a pulse that will activate the warn-away alarm trigger output (not shown) through terminal 85. While this is going on, the circuit remains fully prepared to receive and process other signals from the sensor means 12. In the event a high degree of threat is sensed by sensor means 12 while the warn-away alarm is given, the security breached alarm trigger output, will be tripped through terminal 87 and both alarm outputs will be tripped or triggered simultaneously. In all cases, both alarm trigger outputs are triggered when a high degree of threat is received, unless at the time of the time of threat input, warn-away output is disabled by the bypass timer 143, while only the warn-away alarm trigger output is tripped in response to a low degree of threat.

This invention also carries the capability to drive the vehicle's electronic security system's audible or visual warning devices directly or indirectly by use of an external control relay. Since the warn-away output pulses are short (approximately 200 milliseconds) and could be enabled by the vehicle's electronic security system, this greatly reduces the annoyance created by an alarm system's full alarm. The output drivers have the capability to drive output control circuits as long as a ground is applied to output control terminal 81. These output pulses are fed through output terminals 85 and 87 to directly or indirectly drive warning devices.

FIG. 3 shows an alternate embodiment of the invention. Changing the timing of the full alarm pulse generator 43 to a range greater than the warn-away 200 milliseconds allows for a considerable reduction in the output circuitry. This also reduces the installation time of the present invention. With a 200 millisecond warn-away output pulse and one second full alarm pulse, these pulses can be outputted or multiplexed on the same wire for applying to one such input of the alarm control module. In the same example full alarm output pulse generator 43/timing capacitor 63 is changed to 5 times its normal value. The full alarm output pulse time is therefore increased by a factor of 5.

5,646,591

13

The outputs from output pulse generators 41 and 43 are then applied to the common output indicating LED 69 and output drive transistor 65. This is accomplished through output drive current limiting resistors 67 and 73 and analog bilateral switches 127 and 129 connecting to a common conductor before reaching LED 69. Therefore the LED will indicate warn-away output with a short 200 millisecond light output pulse and full alarm output with a longer one second light output pulse. The output transistor 65 will be conducting, applying a ground or near ground potential to the collector for 200 milliseconds for warn-away and for one second for full alarm.

FIG. 4 represents a modification to the preferred embodiment shown in FIG. 1 and shows the output of the 5 millisecond timer 131 inverting the signal, by inverter 123, and feeding the output signal to two normally open, bilateral switches 100 and 102. The signal closes switches 100 and 102 for the 5 millisecond period. This keeps integrator capacitors 35 and 39 shorted out for the 5 millisecond time period. This represents another method of handling the signal.

FIG. 5 represents a modification to the preferred embodiment shown in FIG. 3 and also shows the output of the 5 millisecond timer 131 to invert the signal, by inverter 123, and feeding the output signal to two normally open, bilateral switches 100 and 102. The signal closes switches 100 and 102 for the 5 millisecond period. This also keeps integrator capacitors 35 and 39 shorted out for the 5 millisecond time period. This represents another method of handling the signal.

FIG. 6 a schematic representation of an alternate embodiment of the of this invention. It is a schematic of a dual stage sensor that uses a custom CMOS integrated circuit (IC). FIGS. 7 through 15 are block diagrams and schematics of this custom CMOS integrated circuit. The schematic in FIG. 6 is the schematic of sensor means 12 being represented by a shock sensor 12. Although this embodiment is hereafter described employing a shock sensor, any sensor could integrate this device.

With the custom IC, there is substantial reduction in the number of parts required to build the product and subsequently the economic cost of the device. The part reduction is evident by the comparison of the part count in the discrete component embodiment of FIG. 5 and the device of the present embodiment shown in FIG. 6. The reduction in component count and their associated cost of assembly, allows for a significant reduction in the cost of the complete sensor unit.

A nominal plus 12.6 volts DC power source enters the sensor at terminal 1 and returns through terminal 11 (common). The current from this power source is limited by current limiting and filtering resistor 5. Capacitor 9 along with resistor 5 filters the transients in the power source. The voltage is then regulated down to 5 volts by resistor 6, zener diode 7, and transistor 8. Transistor 8, zener diode 7, and resistor 6 regulation method was chosen to reduce current in the sensor or to reduce the cost.

Sensor 12 supplies an alternating current (AC) voltage output indicative of the sensed input to the sensor (sound, vibration, shock, movement (field disturbance or ultrasonic sensor), motion, or other input). Sensitivity of the complete sensor is adjusted with potentiometer 23 by adjusting the proportionate input voltage going to IC 201. IC 201 is a CMOS device limiting the frequency input capability of the integrated circuit. This limits the frequency of the RF energy that can enter IC 201 through its input circuitry. Capacitor 24

14

filters low frequency RF energy that may be detected by any of IC 201 input circuitry; therefore, IC 201 eliminates the requirement for having the signal appear, disappear, and then reappear before the sensor will actuate the output. Therefore IC 201 does not include circuitry of the other embodiment which eliminates the DC signal resulting from RF energy feeding into the device.

Resistor 34 establishes a 10 KHz nominal operating frequency of the clock of IC 201. Although IC 201 operates at 5 volts and the maximum operating voltage is 7 volts, the output is protected to 17 volts by stacking the output transistors (not shown) allowing IC 201 to operate in a 12 volt system. Terminal 87 provides a connection for a negative output while triggered on the full alarm output and capacitor 78 provides protection to IC 201 from high voltage transients such as static electricity. LED 69 provides a visual signal of device triggering. In the preferred embodiment it is energized for two seconds. LED 69 will flash at a 5 Hertz rate during a warnaway trigger and is constantly on during the full alarm trigger. The full alarm output signal is negative and the warnaway output is positive. This provides for warnaway output to drive output transistor 65 (required for driving a relay) through base current limiting resistor 67. Transistor 65 then supplies a negative pulse during the warnaway output to output terminal 85. In the preferred embodiment the output pulse is approximately 200 milliseconds for warnaway output and approximately 1.2 seconds for a full alarm output. IC 201 provides both positive and negative voltage outputs to the output terminals as they are required for the application. Another version of this sensor 12 uses two negative outputs from IC 201 to drive alarm inputs directly. The positive output is used to drive a transistor, so that the alarm system can chirp a siren using a relay, with the 200 millisecond warnaway output.

FIG. 7 is a top level block diagram of IC 201 showing its major blocks, digital block 401, analog block 301 and its connection pads. The IC of the preferred embodiment employs eight pins. The logical configuration of this IC has 11 outputs however. Therefore only eight of the eleven pins are brought out in any one configuration. AVSS, the analog ground, is always terminated to VSS, IC 201 ground terminal and its output is not brought out. As stated above, both the full alarm output and the warnaway output have positive and negative pads (pad is an output terminal on the IC chip internal to IC 201), that can be terminated according the requirements of the application. Only one of the full alarm and one of the warnaway alarm outputs are brought out of IC 201.

FIG. 8 is an intermediate level block diagram of analog block 301 showing the major blocks of the analog section of the IC 201, amplifier block 303 and integrator block 305. The basic inputs are shown on the left side and the outputs are shown on the right side of the block diagram. PH1 through PH2B outputs, from the clock of IC 201, drive all the functions of IC 201. VBIAS is a bias for the CMOS analog circuitry of IC 201. PORB is a power on reset (bar or not). VIN is the input signal to amplifier block 303. AVSS is the analog ground reference of IC 201. DISINTEG is a disable the integrator signal from the digital block that uses the amplifier output (AMPOUT) as a clock to initiate the DISINTEG signal. WARNTR is the warnaway trigger output of the warnaway integrator that is used to trigger the timed warnaway output of IC 201. ALARMTR is the full alarm trigger output of the full alarm integrator that is used to trigger the timed full alarm output of IC 201.

FIG. 9 is a schematic/block diagram of amplifier block 303 showing amplifier 307 block, inverting/noninverting

5,646,591

15

determination circuitry and voltage reference circuitry. The inverting/noninverting circuitry provides outputs to effectively rectify the input signal before it is input to the amplifiers. Amplifier 307 block is described in FIG. 10. VREF is established by a voltage divider made up by 190K ohm resistor 315, 5K ohm resistor 317, and 5K ohm resistor 319. VREF is stabilized by 5 picofarad capacitor 313 and micropower amplifier 321 connected as voltage follower. VREF is at 125 millivolts ($(5/200)*5=0.125$). The sensor signal is connected to the input of amplifier 309 which uses VREF as a reference voltage. Amplifier 309 is an inverting switching capacitor amplifier with a gain of 40 that uses clock signals PH1 through PH2B to control the switching of the amplifier signals. A similar amplifier is described below during the disclosure of FIG. 10. The output of amplifier 309 is then input to comparator 311, which is referenced to VREF the same as amplifier 309. Therefore any movement of the IC input signal (sensor output signal) away from its zero reference will cause the output of comparator 311 to go to full output polarity of the signal. This is then input to the "D" input of "D-flip-flop" 323. One of the clock signals, PH1B, is used to clock this to output "Q" on the next clock cycle. PORB control signal resets "D-flip-flop" 323 to a low output at power up. A logic high "Q" output is used as a INV control signal and a logic low signal is inverted by inverter 325 and used as the NONINV control signal.

FIG. 10 is a schematic of amplifier 307 block. It is a pair of switching capacitor amplifiers with a total gain of 1600. During phase 1 of the clock (PH1 and PH1B), analog bilateral switch 335 is open and analog bilateral switches 337, 341, and 349 are closed effectively shorting out both amplifiers 345 and 353, and coupling the signal to the input of the amplifier input capacitor 339 through analog bilateral switch 331, if the signal is not inverted (AVSS (ground) is connected), or analog bilateral switch 333 if the signal is inverted (VIN (input signal) is connected). This places ground at the input and output terminals of both amplifiers 345 and 353, if the input is not inverted, or the level of the signal if the input is inverted. The input signal is very small in amplitude, therefore there is not a significant difference at the output of the second amplifier 353 with either ground or the signal connected.

During phase 2 of the clock (PH2 and PH2B), analog bilateral switch 335 is closed and analog bilateral switches 337, 341, and 349 are open. This connects VIN (input signal) to the input of the amplifiers if the signal is not inverted or connects AVSS (ground) if the signal is inverted. This impresses a positive voltage equal to the input signal across input capacitor 339 (20 picofarads) in either case. If the signal is negative it is inverted by first applying the input signal to amplifiers 345 and 353 while they are shorted and then applying ground to input when they are in the amplifying mode (phase 2). This rectifies the signal by always placing a positive signal, with reference to the applied reference that is applied during the none amplifying mode, to the input of amplifier 345 during the amplifying phase (phase 2 of the clock).

Amplifier 345 has a gain of 40 because it will require 40 times the voltage across 0.5 picofarad capacitor 343 to equalize the input voltage across 20 picofarad capacitor 339. The same is true of amplifier 353 and 20 picofarad capacitor 347 and 0.5 picofarad capacitor 351. Amplifiers 345 and 353 are buffered CMOS micropower amplifiers which are known in the art. Capacitor 354 is a 5 picofarad filter capacitor on the 125 millivolt reference input to amplifiers 345 and 353.

FIG. 11 is a schematic of the warnaway and alarm switching capacitor integrators and their associated circuitry.

16

If the amplifier output signal (AMPOUT) has a fast enough rise time and is of sufficient amplitude to trigger the disable integrator control circuitry (clock a "D-flip-flop"), it will generate a 5 millisecond integrator disable control signal (DISINTEG). This signal will turn on analog bilateral switches 371 and 377, shorting to ground both the warnaway and full alarm integrator capacitors for 5 milliseconds. This will eliminate the first five milliseconds of any high amplitude fast rise time signal, such as one that would be created by the inrush current in a wire going to an incandescent lamp if the wire is near the inductor of an electromagnetic shock sensor. After five milliseconds, the input is allowed to go to the integrator for integration.

During phase 1 (PH1/PH1B) of the clock input capacitor 363 (0.5 picofarad) of the warnaway integrator is shorted to AVSS (ground) on both ends by analog bilateral switches 355 and 367. Also during phase 1 (PH1/PH1B) of the clock input capacitor 365 (0.5 picofarad) of the full alarm integrator is shorted to AVSS (ground) on both ends by analog bilateral switches 359 and 373. During phase 2 (PH2/PH2B) of the clock, integrator input capacitor 363 is connected to the AMPOUT input signal on one end by analog bilateral switch 357 and to warnaway integrator 381 and its associated integration timing control capacitor 379 (10 picofarads) on the other end by analog bilateral switch 369. Additionally, during phase 2 (PH2/PH2B) of the clock, integrator input capacitor 365 is connected to the AMPOUT input signal on one end by analog bilateral switch 361 and to full alarm integrator 385 and its associated integration timing control capacitor 383 on the other end by analog bilateral switch 375. Warnaway integrator 381 would require 20 dumps (20 full clock cycles (2 milliseconds)) of input capacitor 363 into integrator capacitor 379 to equal the average level of the average input signal level. Full alarm integrator 385 would require 200 dumps (200 full clock cycles (20 milliseconds)) of input capacitor 365 (0.5 picofarads) into integrator capacitor 383 (100 picofarads) to equal the average level of the average input signal level. Voltage divider 387 is composed of two equal size CMOS transistors in series, therefore the output of the divider is equal to one half of the VDD voltage of the IC. If VDD is 5 volts, then the reference for comparators 389 and 391 is 2.5 volts. Therefore with an average amplifier output signal level of 2.5 volts into the integrators, it would take 2 milliseconds for warnaway comparator 389 to generate a warnaway trigger output and 20 milliseconds for full alarm comparator 391 to generate a full alarm trigger output. This is in addition to the 5 milliseconds of integrator hold off, if the rise time of the input signal is fast enough and high enough to trigger the disable integrator control signal.

FIG. 12 is an intermediate level block diagram of digital block 401 showing the major blocks of the digital section of the IC, output timer block 403, disable integrator block 405, clock pulse phase circuitry 407, test select 409, RC oscillator 411, power on reset and bias generator 413, and voltage divider 387 disclosed above in the FIG. 11 (integrators). The power on reset and bias generator 413 is a group of transistors and one capacitor that generates a reset at power up and establishes a bias for all the analog amplifiers etc. Resistor capacitor (RC) oscillator 411 has all components on board including a 15 picofarad capacitor, with the exception of the timing resistor, which is external to IC 201. It is a conventional CMOS RC oscillator with a divide by two circuit ("T-flip-flop") to produce a 10 Khz clock from a 20 Khz oscillator. Clock pulse phase circuitry 407 has pulse separation delay circuitry and inverters for both phases of the clock. Test select circuitry 409 selects internal circuits

5,646,591

17

for testing and accelerates the clock for the timers to reduce testing time of the IC. Test is initiated by pulling the input terminal up to VDD and the readings are taken on the adjust terminal.

FIG. 13 is a schematic of output timer block 403. It contains six timer blocks, timer clock divider block 421, and the associated circuitry required to support the output timing of IC 201. The six timers include five divider stages with resets and output determination circuitry. Timer clock divider block 421 has eleven divider stages with resets and a test mode bypass for the first 5 stages to accelerate testing. One of the eleven outputs is used as required for the input clocks to the 6 timers above.

Inverter 423 inverts the negative power on reset (PORB), which is inverted again by inverter 427 before being input to set "D-flip-flop" 431 "Q" output on (high). This starts 1.5 second full alarm disable timer 425 at power up via inverter 433 which inverts the signal to a low, which allows the output of "nor gate" 435 to go high, thereby removing the reset from the timer allowing it to start. When disable timer 425 starts, its done output remains low, which is inverted by inverter 429, thereby continuing to hold the reset off "D-flip-flop" 431, allowing the "Q" output to remain high for the timing cycle of disable timer 425. One and a half second disable timer 425 has a count of 29 with an input clock of 19.53 Hertz, which gives a time of 1.485 seconds, which is very close to the chosen nominal time of 1.5 seconds (1% off). The high "Q" output from "D-flip-flop" 431 is inverted by inverter 433 and used to disable any input from either the warnaway or full alarm integrators. This is done for the full alarm input, by setting the "D" input to "D-flip-flop" 439 low, with the output from inverter 433. This on the next 10 KHz clock cycle sets "D-flip-flop" 439 "Q" output low and holds "D-flip-flop" 437 in reset, thereby not allowing the full alarm input to be clocked through to its output timer 457 for the duration of disable timer 425 timing cycle. For the warnaway input, by setting one of the inputs to AND gate 447 low, forcing AND gate 447 output low disabling "D-flip-flop" 443 by holding it in reset and not allowing the warnaway input to be clocked through to its output timer 473 for the duration of disable timer 425 timing cycle. Full alarm disable timer 425 blocks both warnaway and full alarm inputs.

The positive inverted power on reset (PORB) is also used to reset all other timers. After reset, the alarm trigger input from the full alarm integrator (it triggers at power up) starts two second timer 465 of LED 69, but is blocked from starting full alarm output timer 457 by disable timer 425 holding "D-flip-flop" 437 in reset. Also after reset, the warnaway trigger input from the warnaway integrator (it triggers at power up also) triggers two second warnaway flash timer 483, but is also blocked from triggering warnaway output timer 473 by disable timer 425 holding "D-flip-flop" 443 in reset.

After the 1.5 second period at power on reset, an input from either the full alarm or warnaway integrators will trigger its associated output timers and input disable timer (s). An input from the full alarm integrator will trigger: disable timer 425, full alarm output timer 465 for LED 69, and full alarm output timer 457.

When the trigger is released, alarm disable timer 425 will run its full duration as described above. Full alarm output timer 465 for LED 69 is triggered by setting "RS latch" made up with "nor gates" 469 and 471, then through inverter 467 to release the reset on timer 465 allowing it to start. This will drive LED 69 output continuously for the full duration

18

of the timing cycle through "nor gate" 469 and "or gate" 481 for the duration of timer 465. When timer 465 expires, it resets "RS latch" made up with "nor gates" 469 and 471, which holds the timer in reset and LED 69 off until the input is triggered again. Full alarm output timer 457 is triggered through clocking "D-flip-flop" 437 which transfers the high "D" input to the "Q" output. This sets "RS" latch made up with "nor gates" 461 and 463. The low output from "nor gate" 463 goes to inverter 459 to release the reset on timer 457 allowing it to start. When it starts, it drives the full alarm output through "nor gate" 461 for the full duration of the timing cycle. At the end of the timing cycle, the output of the timer resets "RS latch" made up with "nor gates" 461 and 463, which holds timer 457 in reset and full alarm output off until the full alarm output timer 457 is again triggered by an input from the full alarm integrator.

The warnaway trigger input from the warnaway integrator (shown in FIG. 11) will trigger the following timers of output timer block 403: warnaway disable timer 441 (700 milliseconds in the preferred embodiment), warnaway flash timer 483 for LED 69 (two seconds in the preferred embodiment), and warnaway output timer 473 (200 milliseconds in the preferred embodiment). Warnaway flash timer for LED 69 is started any time the warnaway trigger input is received. The input signal sets "RS latch" made up of "nor gates" 487 and 489. The low output from "nor gate" 489 is inverted by inverter 485. The high signal at the reset input of timer 483 releases the reset and allows timer 483 to start. The low output of timer 483 allows the output of "nor gate" 487 to go high for the duration of the timing cycle. This output is AND-ed with a 5 Hertz clock signal from clock timer 421 by AND gate 491, which will give a 5 Hertz output pulse string for a period of 2 seconds. The 5 Hertz signal is input into "or gate" 481 to drive LED 69 output with the 5 Hertz pulse string for the 2 second period. Hence, LED 69 flashes at a 5 Hertz rate for 2 seconds. A constant 2 second on (high) signal from full alarm output timer 465 of LED 69 will keep LED 69 on constant if it is input to "or gate" 481 at the same time as the 2 second 5 Hertz pulse string is input.

Warnaway output timer 473 is started by the warnaway input from the warnaway integrator clocking the high "D" input to the output. The high "Q" output sets "RS latch" made up of "nor gates" 477 and 479. Then the low output of "nor gate" 479 is inverted by inverter 475, applying a high to the reset input of timer 473. This releases the reset, which allows the timer to start. When warnaway output timer 473 starts, the output goes low, applying a low to one of the inputs of "nor gate" 477. This allows the output to go high, which provides a positive signal to drive the warnaway output, which can either be inverted or not inverted at the output terminal.

The warnaway trigger input clocks the high "D" input of "D-flip-flop" 449 to the "Q" output, the high "Q" output is inverted by inverter 451, providing a low to one of the inputs of "nor gate" 453. This is blocked from releasing the reset on timer 441 by the high warnaway trigger input being high, until the trigger input goes away, at which time warnaway disable timer 441 is started. When timer 441 starts, its output remains low for the duration of the timing cycle. This low output is inverted to a high to continue to hold the reset off on reset input of "D-flip-flop" 449 (it is a negative input for reset). The low output of inverter 451 also goes to the "D" input of "D-flip-flop" 455 which is toggled (transferred) to the "Q" output on the next 10 KHz clock cycle. The low "Q" output of "D-flip-flop" 455 goes to one of the inputs of AND gate 447 forcing its output to go low thereby placing a reset

5,646,591

19

on "D-flip-flop" 443. This blocks any warnaway trigger input to warnaway output timer 473, but does not block a full alarm input, for the duration of the warnaway disable timer 441. When timer 441 times out, its output goes high, producing a low at the output of "nor gate" 445. This resets "D-flip-flop" 449, causing its "Q" output to go low. The low at the "Q" output is inverted by inverter 451, releasing the warnaway trigger input by removing the reset from "D-flip-flop" 443 on the next 10 KHz clock cycle via "D-flip-flop" 455 and AND gate 447. This high at the output of inverter 451 is input to "nor gate" 453 forcing its output to go low. This places a reset on warnaway disable timer 441, forcing its output low. The low at the output of timer 441 is input to "nor gate" 445 allowing its output to go high. This releases the reset on "D-flip-flop" 449, making it available for another warnaway input trigger.

If a warnaway or full alarm input trigger is received while their respective disable timers are running, then that timer is reset by the positive input of the trigger via their respective "nor gates" 435 or 453 (inverts the signal and resets the timer). When the input trigger is removed, the reset is removed allowing the respective timer to start a new timing cycle. Therefore, as long as an activating input is present at the input of IC 201, the respective timer will be held in reset and if the signal goes away and returns within the respective disable timer timing cycle, it will be blocked from generating an output and it will reset and restart the respective disable timer when the signal disappears again.

FIG. 14 is a schematic of the integrator disable control circuit. If during an input, the input rises fast enough and has sufficient amplitude, the AMPOUT (amplifier output) signal will clock the high at "D-flip-flop" 501 "D" input to its "Q" output. This will release the reset on five millisecond integrator disable timer 503, allowing it to start. At the same time the high "Q" output is used to disable both warnaway and full alarm integrators 305 (discussed above). When integrator disable timer completes its cycle, its output goes high setting "RS latch" made up of "nor gates" 505 and 507. When the "RS latch" is set, a high out of "nor gate" 507 goes to "nor gate" 513, forcing its output to go low, resetting integration minimum time timer 515. One half of a 5 KHz clock cycle later (the Clock is inverted by inverter 509), a high input to "nor gate" 507 resets the "RS latch" and forces "nor gate" 507 output low, allowing the output of "nor gate" 513 to go high thereby releasing timer 515 to start its timing cycle. When integration minimum time timer 515 is reset or is in its timing cycle, its output is low, placing a reset on "D-flip-flop" 501 and disabling any additional integrator disable output for the duration of the reset and the timer's timing cycle, which is 400 milliseconds. PORB (power on reset bar or not) is inverted by inverter 511. The high reset signal out of inverter 511 then resets the "RS" latch and integration minimum time timer 515, starting a 400 millisecond timing cycle at power on reset.

FIG. 15 is a schematic of one of the 5 stage "T-flip-flop" timers that is used in IC 201. Any number of clock cycles can be used in these timers up to 31 (2^5-1), which is the number that is used in the FIG. 15 schematic. Unless the timing hits right on for a low count, it is preferable to use a higher count for better accuracy in the timing which provides for higher resolution. The 5 stage timers can use any output from clock divider timer 421. Warnaway output timer 473 with its 5 stage timing using a 5 KHz clock from divider timer 421 would have a time-out or a complete cycle of 6.2 milliseconds, while using a 5 Hertz output would have a time-out of 6.35 seconds.

Warnaway output timer 473, using a 156.25 Hertz clock input at the "T" input would have a 198.4 milliseconds

20

time-out (within 1% of the nominal 200 milliseconds chosen). When the RB (reset bar) input is low, the timer is held off with all of the QB's ("Q" bars) high. When the reset is released and a clock signal is input at the "T" input to "or gate" 525, the output of "or gate" 525 will follow the clock until "done" goes high forcing "or gate" 525 to remain high as long as "done" is high, thereby stopping and holding the count at 31 until the timer is reset and released from reset. Each "T-flip-flop" stage divides the clock by 2. After "T-flip-flop" 527, the clock frequency would be 78.125 Hertz. After "T-flip-flop" 529, the clock frequency would be 39.0625 Hertz. After "T-flip-flop" 531, the clock frequency would be 19.53125 Hertz. After "T-flip-flop" 533, the clock frequency would be 9.765625 Hertz. After the last stage "T-flip-flop" 535 the clock frequency would be 4.8828125 Hertz if the counter would continue to run, but when all of the "QB" outputs go low, all the inputs to "nor gate" 537 are low, thereby allowing the "done" output to go high which blocks the clock input and stops counter/timer with a count of 31. It will remain stopped until the timer is reset and the reset is released.

Also this unit is described as a 2-stage sensor, but the invention is not limited to 2 stages and may be employed with three (3) or more stages (where a stage is level of threat input generating a predetermined alarm response). The output pulses may vary in lengths such as 200 milliseconds for the "warn-away" and approximately one full second for the full alarm output. This will allow alarms with the capability to distinguish between "warn-away" and full alarm with one input. This also provides for elimination of one drive transistor and one wire.

The above disclosure makes reference to component values and to time values. This is provided to aid the reader in reconstruction and understanding of the circuit. However, it is not limiting to the invention. A number of values may be employed to achieve the same or substantially the same result and to vary the parameters of the application.

While the invention has been described by reference to a particular embodiment thereof, those skilled in the art will be able to make various modifications to the described embodiment of the invention without departing from the true spirit and scope thereof. It is intended that all combinations of elements and steps which perform substantially the same function in substantially the same way to achieve the same results are within the scope of this invention.

What is claimed is:

1. A method of indicating a degree of incoming threat to an electronically secured area comprising the steps of:

- sensing via a sensor means a degree of threat delivered to a secured area;
- generating from the output of said means an electric signal proportional to said degree of threat;
- analyzing said signal to determine if it represents a low degree of threat or a high degree of threat; and
- producing either a first pulse representing said low degree of threat or separately producing said first pulse and a second pulse representing a signal having both said low degree of threat and said high degree of threat.

2. The method of claim 1 wherein said sensor means is chosen from a group consisting of shock sensors, motion sensors, field disturbance sensors, sound discriminator sensors, ultrasonic sensors and current sensors.

3. The method of claim 2 wherein the step of generating said electric signal includes the step of generating an alternating current signal whose amplitude is proportional to said degree of threat.

5,646,591

21

4. The method of claim 2 wherein the step of analyzing said signal includes the steps of:

- a) amplifying said signal to produce an amplified signal;
- b) impressing said amplified signal simultaneously to at least two separate integrators of different sensitivity to produce integrated signals; and
- c) activating a pulse generator specific to each said integrated signal if the associated integrated signal reaches a predetermined level.

5. The method of claim 4 wherein the step of analyzing said signal further includes the steps of:

- a) impressing said integrated signals simultaneously to respective comparators of different sensitivity to produce a first comparator signal if the associated integrated signal reaches a first predetermined level indicating said low degree of threat signal or a second comparator signal if the associated integrated signal reaches a second, higher predetermined level indicating said high degree of threat signal; and
- b) activating a pulse generator specific to said first and said second comparator signals.

6. The method of claim 2 wherein the step of analyzing said signal includes the steps of:

- a) amplifying said signal to produce an amplified signal;
- b) impressing said amplified signal simultaneously to at least two separate integrators/comparators, each said integrator/comparator having different sensitivity; and
- c) activating a pulse generator to produce said first and said second pulses specific to each signal integrated and compared if that signal reaches an associated predetermined level.

7. The method of claim 2 wherein said step of analyzing said signal includes the steps of:

- a) amplifying said signal with an amplifier to produce an amplified signal;
- b) impressing said amplified signal simultaneously to at least two separate integrators of different sensitivity to produce integrated amplified signals;
- c) separately impressing said integrated, amplified signals to at least two signal comparators, one in series with each integrator and of different sensitivity, to provide a first comparator signal indicating said low degree of threat or a second comparator signal indicating said high degree of threat if the integrated, amplified signal reaches an associated predetermined level; and
- d) activating a pulse generator specific to each said comparator signal.

8. The method of claim 2 including the additional step of ignoring said signal produced by said sensor means for a predetermined amount of time to eliminate spurious, non-physical signals interacting with said sensor means.

9. The method of claim 8 wherein the step of ignoring said signal includes the step of opening a normally closed switch to disconnect said amplified signal, for said predetermined amount of time to eliminate spurious, nonphysical signals produced by random energy fields interacting with said sensor means.

10. The method of claim 8 wherein the step of ignoring said signal for said predetermined amount of time includes the step of opening a pair of normally closed switches for preventing second pulses from being output to an alarm controller to eliminate signals produced by continuous energy fields interacting with said sensor means.

11. The method of claim 8 wherein the step of ignoring said signal for said predetermined amount of time includes

22

the step of resetting a flip-flop having an output therein and generating a logic low output for preventing the production of said first and said second pulses to eliminate signals produced by continuous energy fields interacting with said sensor means.

12. The method of claim 8 wherein said nonphysical signals include an EMF signal or an RF signal.

13. The method of claim 1 including the additional step of ignoring any signal that does not disappear and later reappear.

14. The method of claim 13 wherein said step of ignoring a signal that does not disappear and later reappear includes the steps of triggering a first or second timer to generate a third or a fourth pulse for opening a respective normally closed switch to prevent providing said first or second pulses to an alarm controller.

15. The method of claim 14 wherein said step of ignoring a signal that does not disappear and later reappear includes the steps of triggering said first or said second timer to generate said third or said fourth pulses for opening of respective normally closed switches to prevent providing said first or second pulses to said alarm controller for the duration of said threat delivered to said secured area.

16. The method of claim 1 further including the step of sending said pulses over a single conductor to an alarm controller.

17. The method of claim 16 wherein said alarm system controller recognizes said pulses by their associated pulse-width as either a full alarm threat or a warn-away threat.

18. An electronic security system for indicating a degree of threat incoming to an electronically secured area comprising:

- a) sensor means for sensing a degree of threat delivered to a protected area;
- b) means for generating an electric signal proportional to said degree of threat;
- c) means for analyzing said electric signal to determine if it represents a low degree of threat or a high degree of threat; and
- d) means for producing either a first pulse, representing said low degree of threat, or means for separately producing said first pulse and a second pulse, representing said signal having both said low degree of threat and said high degree of threat.

19. The device of claim 18 wherein said sensor means is chosen from a group consisting of shock sensors, motion sensors, field disturbance sensors, sound discriminator sensors, ultrasonic sensors and current sensors.

20. The device of claim 19 further including means for ignoring said signal produced by said sensor means for a predetermined amount of time to eliminate spurious, non-physical signals.

21. The device of claim 20 wherein the means for ignoring said signal includes a normally closed switch which is opened for said predetermined amount of time for disconnecting said signal to thereby eliminate spurious, nonphysical signals produced by random energy fields interacting with said sensor means.

22. The device of claim 20 wherein means for ignoring said signal includes a pair of normally closed switches for preventing providing said first and said second pulses for said predetermined amount of time to an alarm controller to eliminate signals produced by continuous energy fields interacting with said sensor means.

23. The device of claim 20 wherein means for ignoring said signal includes a flip-flop having an output therein for generating a logic low output for preventing providing said

5,646,591

23

first and said second pulses for said predetermined amount of time to an alarm controller for eliminating signals produced by continuous energy fields interacting with said sensor means.

24. The device of claim 20 wherein said nonphysical signals include an EMF signal or an RF signal.

25. The device of claim 18 further including means for ignoring any signal that does not disappear and later reappear.

26. The device of claim 25 wherein said means for ignoring a signal that does not disappear and later reappear includes a first or second timer for generating a third or a fourth pulse for opening respective normally closed switches to prevent providing said first or second pulses to an alarm controller.

27. The device of claim 26 wherein said means for ignoring a signal that does not disappear and later reappear triggers said first or said second timer to generate said third or said fourth pulses for opening said normally closed switches to prevent providing said first or second pulses to said alarm controller for the duration of said threat delivered to said secured area.

28. The device of claim 18 further including a single conductor sending said first and second pulses to an alarm controller.

29. The device of claim 28 further including an alarm system controller for recognizing said pulses by their associated pulsewidth as either a full alarm threat or a warn-away threat.

30. The device of claim 18 further including a capacitor through which said signal is passed to remove any direct current and voltage therefrom.

31. The device of claim 18 wherein said means for analyzing said signal includes:

- a) a signal amplifier, having an input and an output therein, for receiving said signal from said sensor means and producing an amplified signal thereof; and
- b) a first and second voltage integrator connected to said amplifier output, said first integrator having a high sensitivity for responding to said low degree of threat signal and said second integrator having a lower sensitivity for responding to said high degree of threat signal, said integrators simultaneously receiving said amplified signal from said amplifier.

32. The device of claim 18 wherein said means for analyzing said signal includes:

- a) a signal amplifier, having an input and an output therein, for receiving said signal from said sensor means and producing an amplified signal thereof; and
- b) a pair of voltage comparators connected to said amplifier output, said first comparator having a high sensitivity for responding to said low degree of threat signal and said second comparator having a lower sensitivity for responding to said high degree of threat signal, said comparators simultaneously receiving said amplified signal from said amplifier.

33. The device of claim 18 wherein said means for analyzing said signal includes:

- a) a signal amplifier, having an input and an output therein, for receiving said signal from said sensor means and producing an amplified signal thereof; and
- b) a first and second voltage integrator and comparator connected to said amplifier output, said first integrator-comparator having a high sensitivity for responding to said low degree of threat signal and second said integrator-comparator having a lower sensitivity for

24

responding to said high degree of threat signal said integrators and comparators simultaneously receiving said amplified signal from said amplifier.

34. The device of claim 18 wherein said means for producing either said first pulse or said separate first and second pulses includes a first and second voltage comparator/output-pulse-generator, each connected to a respective voltage integrator for comparing integrated voltages produced from each said integrator and producing said first pulse representing said low degree of threat signal from a high sensitivity integrator and separately producing both said first and said second pulse representing said low degree of threat signal from said high sensitivity integrator and said high degree of threat signal from a low sensitivity integrator.

35. The device of claim 34 further including a single conductor coupled to outputs of said pulse generators for transmission of said first and said second pulses having different pulsewidths.

36. The device of claim 18 further including a single conductor for transmission of said first and said second pulse therethrough.

37. The device of claim 18 wherein said first and said second pulses have a first and a second pulsewidth.

38. The device of claim 37 wherein said first pulsewidth is greater than said second pulsewidth or said second pulsewidth is greater than said first pulsewidth.

39. A method of blocking undesirable signals from activation of an alarm in an electronically secured area comprising the steps of:

- a) sensing via a sensor means a degree of threat delivered to a protected area;
- b) generating from the output of said sensor means an electric signal, having strength proportional to said degree of threat;
- c) amplifying said signal to produce an amplified signal;
- d) deleting the front end of said amplified signal and removing it from further consideration;
- e) inputting said amplified signal to a comparator for comparing said amplified signal against a known reference;
- f) producing in response to said comparison either a first pulse, representing a low degree of threat, or separately producing said first pulse and a second pulse, representing a signal having both said low degree of threat and a high degree of threat; and
- g) simultaneously preventing the output of either said separate first and second pulses or said first pulse to an alarm until said amplified signal disappears and later reappears.

40. The method of claim 39 wherein said sensor means is chosen from a group consisting of shock sensors, motion sensors, field disturbance sensors, sound discriminator sensors, ultrasonic sensors and current sensors.

41. The method of claim 40 wherein the step of amplifying said signal includes the additional steps of amplifying and rectifying a full wave of said signal so that said amplified signal represents all values of said signal, is solely positive, and reduces the differential in the positive and negative aspects of said signal.

42. The method of claim 40 including the additional step of ignoring said signal produced by said sensor means for a predetermined amount of time to eliminate spurious, non-physical signals interacting with said sensor means.

43. The method of claim 42 wherein the step of ignoring said signal includes the step of opening a normally closed switch to disconnect said amplified signal, for said prede-

5,646,591

25

terminated amount of time, to eliminate spurious, nonphysical signals produced by random energy fields interacting with said sensor means.

44. The method of claim 42 wherein the step of ignoring said signal for said predetermined amount of time includes the step of opening a pair of normally closed switches to prevent said first and second pulses from being output to an alarm controller to eliminate signals produced by continuous energy fields interacting with said sensor means.

45. The method of claim 42 wherein the step of ignoring said signal for said predetermined amount of time includes the step of resetting a flip-flop having an output therein and generating a logic low output for preventing production of said first and said second pulses to eliminate signals produced by continuous energy fields interacting with said sensor means.

46. The method of claim 42 wherein said nonphysical signals include an EMF signal or an RF signal.

47. The method of claim 40 further including the step of ignoring any signal that does not disappear and later reappear.

48. The method of claim 47 wherein said step of ignoring a signal that does not disappear and later reappear includes triggering a first or second timer to generate a third or a fourth pulse for opening of an associated normally closed switch to thereby prevent said first or second pulses from being output to an alarm controller.

49. The method of claim 48 wherein said step of ignoring a signal that does not disappear and later reappear includes the steps of triggering said first or said second timer to generate said third or said fourth pulses for opening of said normally closed switches to thereby prevent said first or second pulses from being output to said alarm controller for the duration of said threat delivered to said secured area.

50. The method of claim 39 employing a single conductor for transmission of said first and said second pulse there-through.

51. The method of claim 39 employing a single conductor coupled to outputs of a pair of pulse generators generating said first and second pulses for transmission of said first and said second pulses having different pulsewidths.

52. The method of claim 39 wherein said first and said second pulses have a first and a second pulsewidth.

53. The method of claim 52 wherein said first pulsewidth is greater than said second pulsewidth or said second pulsewidth is greater than said first pulsewidth.

54. A method of indicating a degree of an incoming threat to an electronically secured area comprising the steps of:

- a) sensing via a sensor means a degree of threat delivered to an electronically secured area including the step of generating an alternating current signal whose amplitude is proportional to said degree of threat;
- b) analyzing said signal to determine if it is of a low, degree of threat or of a high degree of threat, including the steps of:
 - i) rectifying and amplifying said signal;
 - ii) impressing the resulting rectified, amplified signal simultaneously to at least two separate integrators of different sensitivity;
 - iii) impressing the resulting separate integrated, amplified signals to at least two signal comparators of different sensitivity, one in series with each of said integrators; and
 - iv) activating at least one pulse generator responsive to an output of each said signal comparator; and
- d) producing either a first pulse representing said low degree of threat or separately producing said first and a

26

second pulse representing a signal having both said low degree and said high degree of threat.

55. The method of claim 54 wherein said sensor means is chosen from a group consisting of shock sensors, motion sensors, field disturbance sensors, sound discriminator sensors, ultrasonic sensors and current sensors.

56. The method of claim 54 including the additional step of ignoring said signal produced by said sensor means for a predetermined amount of time to eliminate spurious, nonphysical signals interacting with said sensor means.

57. The method of claim 56 wherein the step of ignoring said signal includes the step of opening a normally closed switch to disconnect said amplified signal, for said predetermined amount of time, from said integrators to eliminate spurious, nonphysical signals produced by random energy fields interacting with said sensor means.

58. The method of claim 56 wherein the step of ignoring said signal for said predetermined amount of time includes the step of opening a normally closed pair of switches to disconnect said pulse generators and prevent said first and second pulses from being output to an alarm controller to eliminate signals produced by continuous energy fields interacting with said sensor means.

59. The method of claim 56 wherein the step of ignoring said signal for said predetermined amount of time includes the step of resetting a flip-flop having an output therein and generating a logic low output for preventing said first and said second pulses from said pulse generators from being output to an alarm controller to eliminate signals produced by continuous energy fields interacting with said sensor means.

60. The method of claim 56 wherein said nonphysical signals include an EMF signal or an RF signal.

61. The method of claim 54 including the step of ignoring any signal that does not disappear and later reappear.

62. The method of claim 61 wherein said step of ignoring a signal that does not disappear and later reappear includes the steps of triggering a first or second timer to generate a third or a fourth pulse for opening of an associated normally closed switch to thereby prevent said first or second pulses from being output to an alarm controller.

63. The method of claim 62 wherein said step of ignoring a signal that does not disappear and later reappear includes the steps of triggering said first or said second timer to generate said third or said fourth pulses for opening of said normally closed switches to thereby prevent said first or second pulses from being output to said alarm controller for the duration of said threat delivered to said secured area.

64. The method of claim 63 further including the step of an alarm system controller recognizing said pulses by their associated pulsewidth as either a full alarm threat or a warn-away threat.

65. The method of claim 62 wherein the step of producing either said first pulse or said second pulse includes sending said pulses over a single conductor to an alarm controller.

66. An electronic security system for indicating a degree of threat incoming to an electronically secured area comprising:

- a) sensor means for sensing a degree of threat delivered to a secured area having the capability of outputting an electric signal having strength proportional to said degree of threat;
- b) a capacitor through which said signal is passed to remove any direct current and voltage therefrom;
- c) means for analyzing said signal to determine if it represents a low degree of threat or a high degree of threat including:

5,646,591

27

- i) a signal amplifier for receiving said signal from said sensor means; and
- ii) a pair of voltage integrators connected to an output of said amplifier, one said integrator having a high sensitivity for responding to a low intensity amplified signal and the other said integrator having a lower sensitivity for responding to a higher intensity amplified signal and for simultaneously receiving said amplified signal from said amplifier; and
- d) means for producing either separate first and second pulses representing a signal containing both a low degree of threat and a high degree of threat, or said first pulse representing said low degree of threat including a pair of voltage comparators/output-pulse-generators, one connected to each said voltage integrator for comparing outputs produced from each said integrator and for producing a first pulse representing said low degree of threat from said high sensitivity integrator and for producing both said first and said separate second pulse from both said generators representing said low degree of threat from said high sensitivity integrator and said high degree of threat from said low sensitivity integrator.
67. The system of claim 66 wherein said sensor means is chosen from a group consisting of shock sensors, motion sensors, field disturbance sensors, sound discriminators, ultrasonic sensors and current sensor.
68. The system of claim 67 wherein said signal produced by said sensor means is ignored for a predetermined amount of time to eliminate spurious, nonphysical signals interacting with said sensor means.
69. The system of claim 68 wherein a normally closed switch is opened to disconnect said amplified signal, for said predetermined amount of time, from said integrators to eliminate spurious, nonphysical signals produced by random energy fields interacting with said sensor means.
70. The system of claim 68 wherein a normally closed pair of switches are opened to disconnect said first and said second pulse generators and to thereby prevent said first and second pulses from being output to an alarm controller to eliminate signals produced by continuous energy fields interacting with said sensor means.
71. The system of claim 68 wherein a flip-flop having an output therein is reset to generate a logic low output to disconnect said pulse generators and to eliminate signals produced by continuous energy fields interacting with said sensor means.
72. The system of claim 68 wherein said nonphysical signals include an EMF signal or an RF signal.
73. The system of claim 66 wherein any signal that does not disappear and later reappear is ignored.
74. The system of claim 73 wherein ignoring a signal that does not disappear and later reappear is accomplished by triggering a first or second timer to generate a third or a fourth pulse to open a normally closed associated switch to thereby prevent said first or second pulses from being output to an alarm controller.
75. The system of claim 74 wherein ignoring a signal that does not disappear and later reappear is accomplished by triggering said first or said second timer to generate said third or said fourth pulse to open said normally closed associated switch to thereby prevent said first or second pulse from being output to said alarm controller for the duration of said threat delivered to said secured area.
76. The system of claim 66 wherein said pulses are sent over a single conductor to an alarm controller.
77. The system of claim 66 wherein an alarm system controller recognizes said pulses by their associated pulse-width as either a full alarm threat or a warn-away threat.

28

78. A method of indicating a degree of incoming threat to an electronically secured area comprising the steps of:
- sensing via a sensor means a degree of threat delivered to a secured area, said sensor means generating an electric signal proportional to said degree of threat;
 - analyzing said signal to determine if it represents a low degree of threat or a high degree of threat; and
 - producing either a first pulse representing said low degree of threat or separately producing said first pulse and a second pulse representing a signal having both said low degree of threat and said high degree of threat.
79. The method of claim 78 wherein said sensor means is chosen from a group consisting of shock sensors, motion sensors, field disturbance sensors, sound discriminator sensors, ultrasonic sensors and current sensors.
80. The method of claim 79 wherein said electric signal is an alternating current signal whose amplitude is proportional to said degree of threat.
81. The method of claim 79 wherein the step of analyzing said signal includes the steps of:
- amplifying said signal to produce an amplified signal;
 - impressing said amplified signal simultaneously to at least two separate integrators to produce integrated signals; and
 - activating a pulse generator specific to each said integrated signal if the associated integrated signal reaches a predetermined level.
82. The method of claim 79 wherein the step of analyzing said signal further includes the steps of:
- amplifying said signal to produce an amplified signal;
 - impressing said amplified signal simultaneously to at least two separate comparators of different sensitivity to produce a first comparator signal if the associated integrated signal reaches a first predetermined level indicating said low degree of threat signal or a second comparator signal if the associated integrated signal reaches a second, higher predetermined level indicating said high degree of threat signal; and
 - activating a pulse generator specific to said first and said second comparator signals.
83. The method of claim 79 wherein the step of analyzing said signal includes the steps of:
- amplifying said signal to produce an amplified signal;
 - impressing said amplified signal simultaneously to at least two separate integrators/comparators, each said integrator/comparator having different sensitivity; and
 - activating a pulse generator specific to each said integrator/comparator to produce said first and/or said second pulse if the respective output signal reaches a predetermined level.
84. The method of claim 79 wherein said step of analyzing said signal includes the steps of:
- amplifying said signal with an amplifier to produce an amplified signal;
 - impressing said amplified signal simultaneously to at least two separate integrators of different sensitivity to produce integrated amplified signals;
 - separately impressing said integrated, amplified signals to at least two signal comparators, one in series with each integrator and of different sensitivity, to provide a first comparator signal indicating said low degree of threat or a second comparator signal indicating said high degree of threat if the integrated, amplified signal reaches an associated predetermined level; and

d) activating a pulse generator specific to each said comparator signal.

85. The method of claim 79 including the additional step of ignoring said signal produced by said sensor means for a predetermined amount of time to eliminate spurious, non-physical signals interacting with said sensor means.

86. The method of claim 85 wherein the step of ignoring said signal includes the step of closing normally open first and second switches to prohibit processing of said signal for a predetermined amount of time to eliminate spurious, nonphysical signals produced by random energy fields interacting with said sensor means.

87. The method of claim 85 wherein the step of ignoring said signal for said predetermined amount of time includes the step of opening normally closed switches, thereby preventing said first and second pulses from being output to an alarm controller to eliminate signals produced by continuous energy fields interacting with said sensor means.

88. The method of claim 85 wherein the step of ignoring said signal for said predetermined amount of time includes the step of resetting a flip-flop having an output therein and generating a logic low output for preventing said first and said second pulses from being output to an alarm controller to eliminate signals produced by continuous energy fields interacting with said sensor means.

89. The method of claim 85 wherein said nonphysical signals include an EMF signal or an RF signal.

90. The method of claim 78 including the additional step of ignoring any signal that does not disappear and later reappear.

91. The method of claim 90 wherein said step of ignoring a signal that does not disappear and later reappear includes the steps of triggering a first or second timer to generate a third or a fourth pulse for opening of a normally closed switch to thereby prevent said first or second pulses from being output to an alarm controller.

92. The method of claim 91 wherein said step of ignoring a signal that does not disappear and later reappear includes the steps of triggering said first or said second timer to generate said third or fourth pulses for opening of said normally closed switches to thereby prevent said first or second pulses from being output to said alarm controller for the duration of said threat delivered to said secured area.

93. The method of claim 78 further including the step of sending said pulses over a single conductor to an alarm controller.

94. The method of claim 93 wherein an alarm system controller recognizes said pulses by their associated pulse-width as either a full alarm threat or a warn-away threat.

* * * * *



US00D345711S

United States Patent [19]

[11] Patent Number: Des. 345,711

Issa

[45] Date of Patent: ** Apr. 5, 1994

- [54] VEHICLE ALARM CASE MODULE
- [76] Inventor: Darrell E. Issa, 1598 Parkview Dr., Vista, Calif. 92083
- [**] Term: 14 Years
- [21] Appl. No.: 3,712
- [22] Filed: Jan. 15, 1993
- [52] U.S. Cl. D10/106
- [58] Field of Search 340/540, 546, 565, 568, 340/571, 572, 573, 574, 541, 542, 584; 116/169; D10/104, 106, 116, 121

Assistant Examiner—Marcus Jackson
Attorney, Agent, or Firm—John J. Murphey

[57] CLAIM

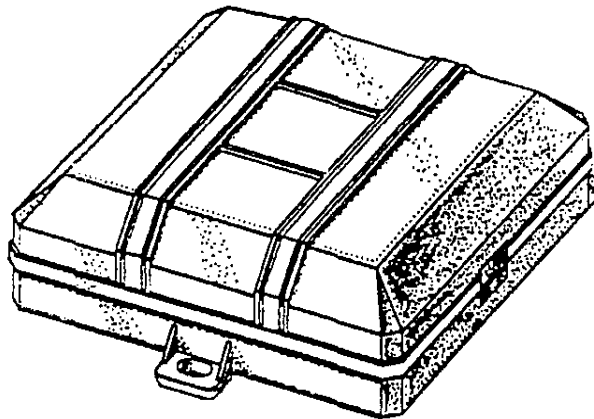
The ornamental design of a vehicle alarm case module, as shown and described.

DESCRIPTION

FIG. 1 is a top plan view of the vehicle alarm case module showing my new design;
 FIG. 2 is a bottom plan view of the device showing my new design;
 FIG. 3 is a left side elevational view thereof showing the design;
 FIG. 4 is a right side elevational view thereof showing my new design;
 FIG. 5 is a front elevational view of my new design;
 FIG. 6 is a rear elevational view of the vehicle alarm case module; and,
 FIG. 7 is a trimetric view thereof showing my new design.

- [56] **References Cited**
- U.S. PATENT DOCUMENTS**
- D. 303,223 9/1989 Issa D10/106
- D. 333,633 3/1993 Issa D10/106
- D. 333,634 3/1993 Issa D10/106
- D. 333,996 3/1993 Matt et al. D10/106

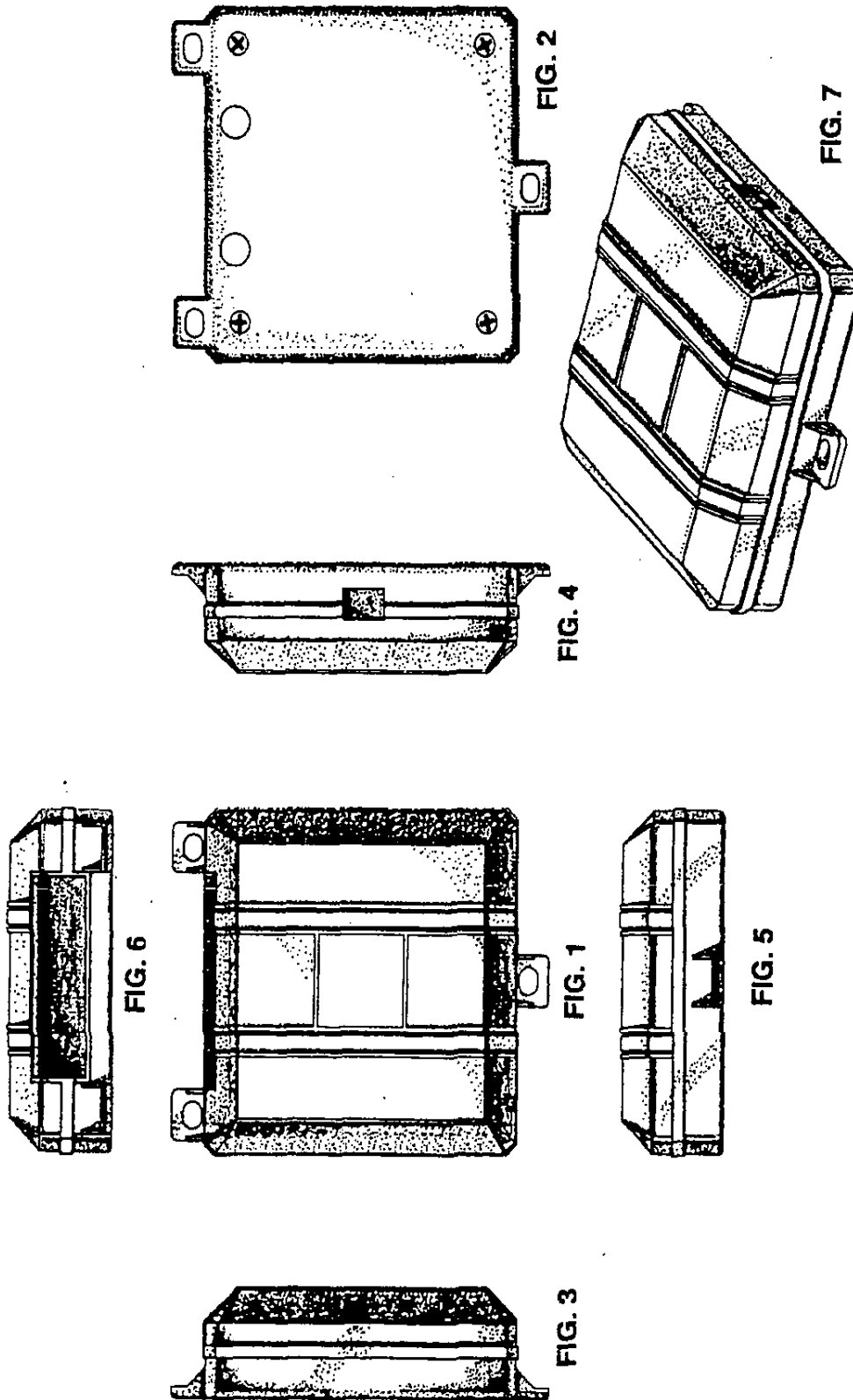
Primary Examiner—Wallace R. Burke



U.S. Patent

Apr. 5, 1994

Des. 345,711



United States Patent [19]

[11] Patent Number: 4,584,569

Lopez et al.

[45] Date of Patent: Apr. 22, 1986

[54] MOTION SENSITIVE SECURITY SYSTEM

[56]

References Cited

[76] Inventors: Michael J. Lopez, 970 Calle Venado, Anaheim, Calif. 92807; Howard A. Williams, Jr., 2629 X. Griset Pl., Santa Ana, Calif. 92704; Henry J. Salvatori, 10633 Virginia Ave., Whittier, Calif. 90603

U.S. PATENT DOCUMENTS

- 4,180,811 12/1979 Yoshimura et al. 340/566
- 4,234,876 11/1980 Murai 340/566
- 4,418,337 11/1983 Bader 340/566

Primary Examiner—Glen R. Swann, III
Attorney, Agent, or Firm—Grover A. Frater

[21] Appl. No.: 650,835

[57] ABSTRACT

[22] Filed: Sep. 17, 1984

The preferred arrangement utilizes a magnet suspended at the center of an elastic cord over a pickup coil. Movement of the magnet is sensed by the coil in that signals are generated by such movement. The signals are processed in the combination of a time delay circuit and a comparator to provide an output which is a measure of acceleration of the element on which the elastic cord is mounted and, in one form, by a measure of jerk in a similar time delay circuit and comparator combination.

Related-U.S. Application Data

[63] Continuation-in-part of Ser. No. 324,170, Nov. 23, 1981, abandoned.

[51] Int. Cl.⁴ G08B 21/00

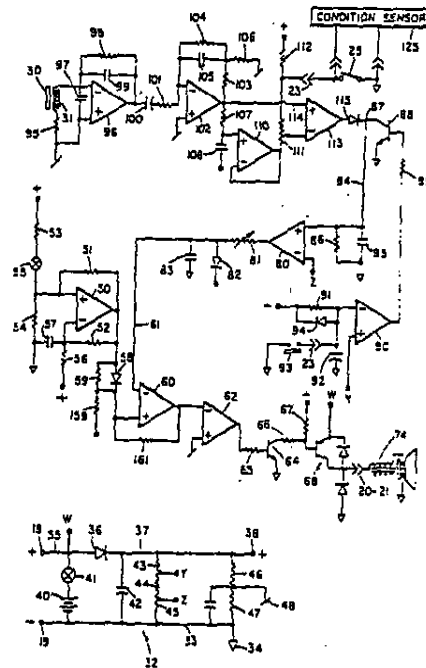
[52] U.S. Cl. 340/566; 73/650;

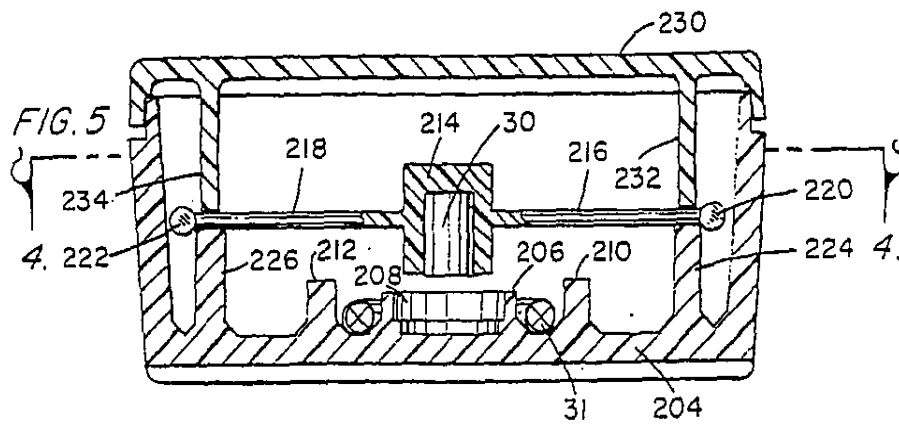
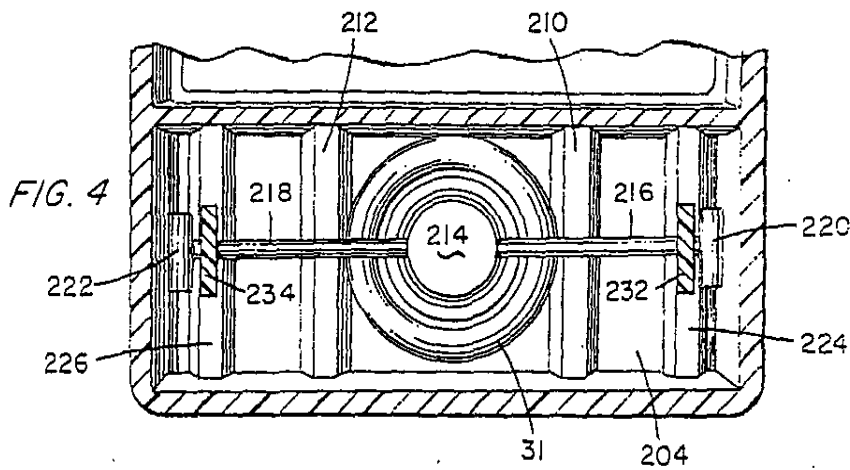
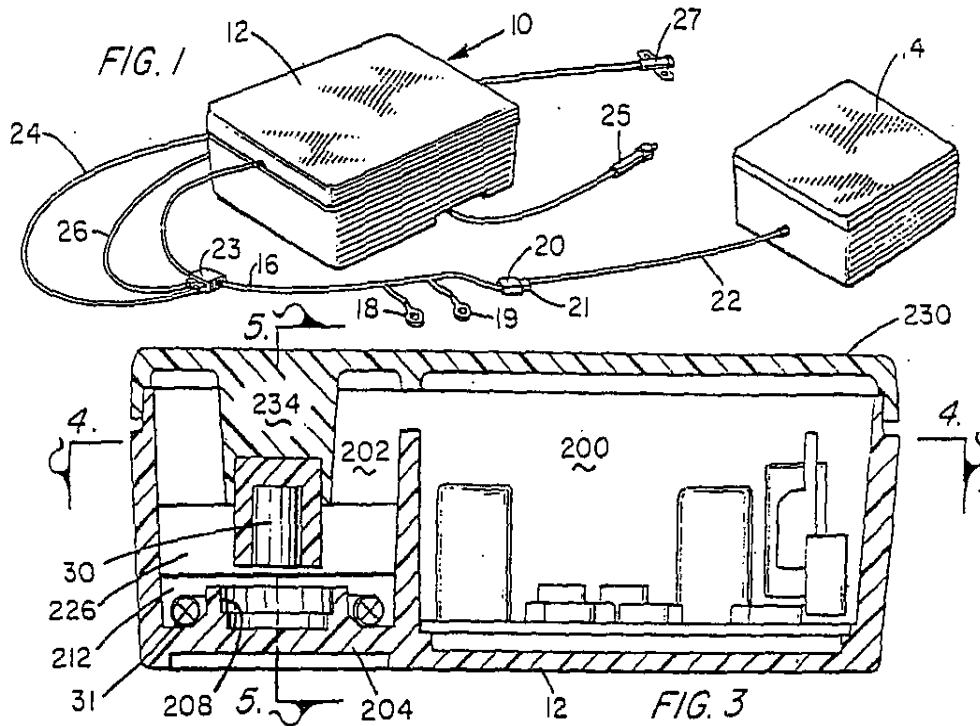
73/654; 340/65; 340/571

[58] Field of Search 340/566, 65, 571;

73/654, 650, 658

22 Claims, 6 Drawing Figures





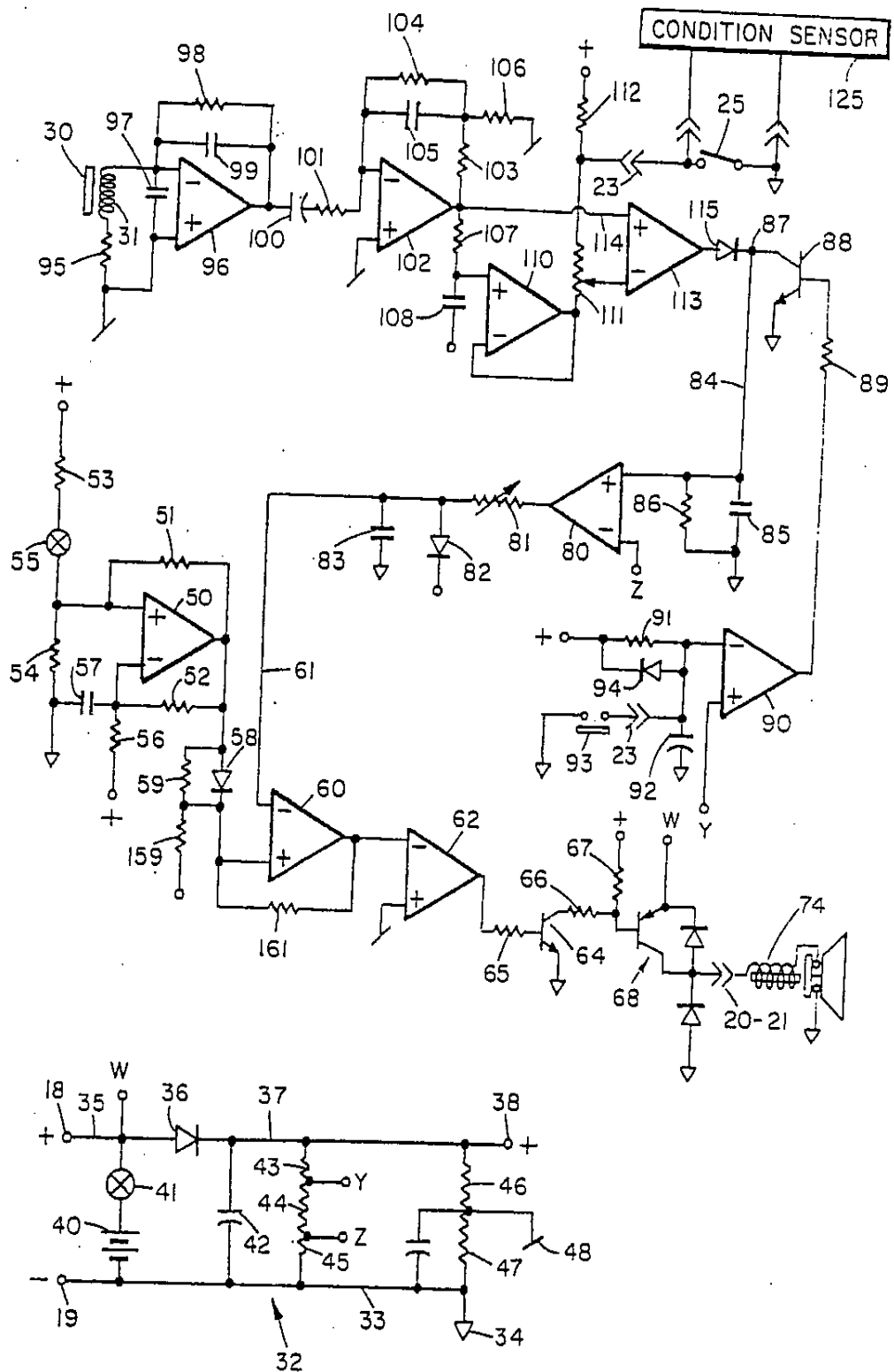
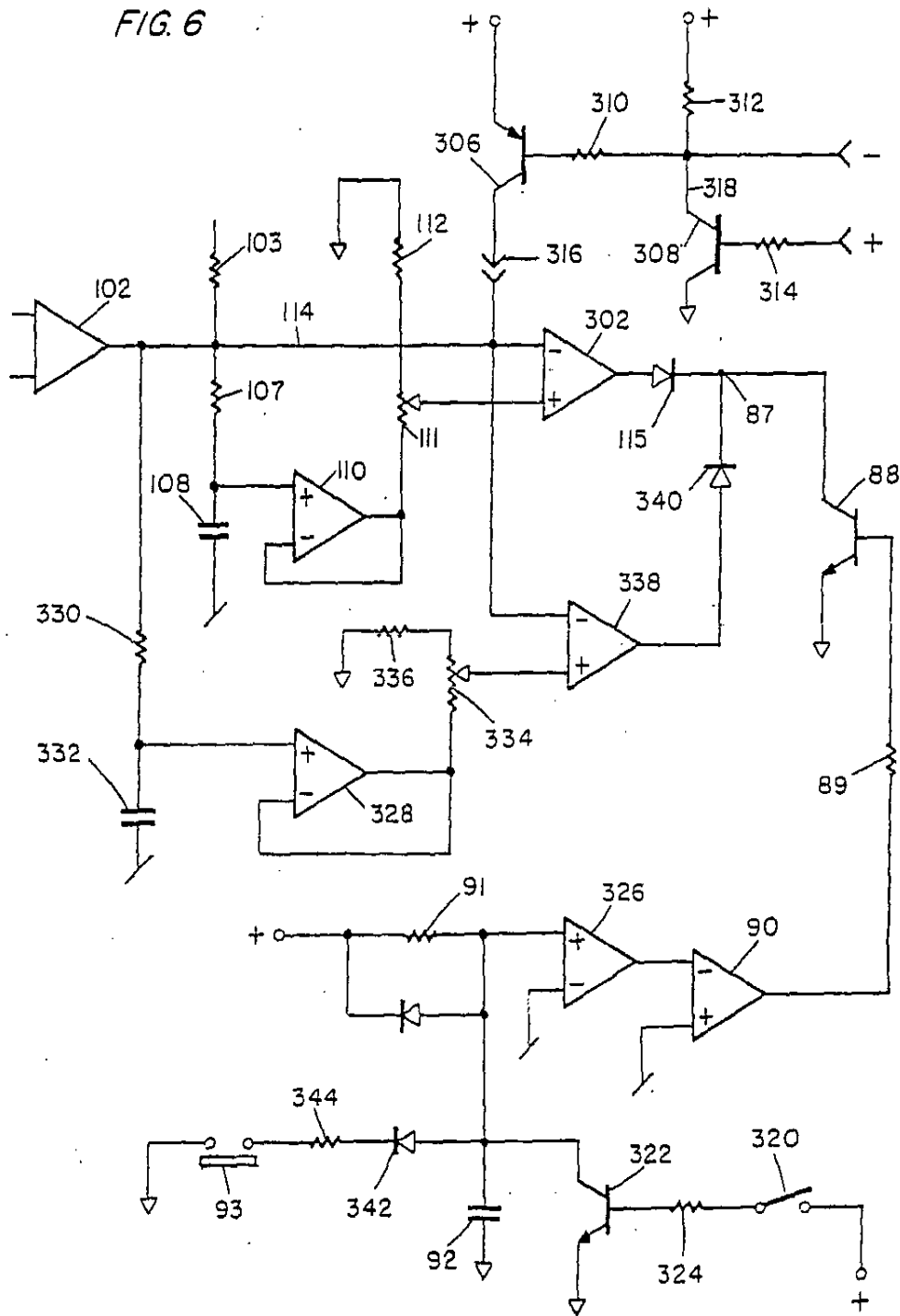


FIG. 2

FIG. 6



MOTION SENSITIVE SECURITY SYSTEM

CROSS-REFERENCE TO RELATED APPLICATION

This application is a continuation-in-part of application Ser. No. 06/324,170, filed Nov. 23, 1981, now abandoned.

TECHNICAL FIELD

This invention relates to security systems generally and to improved motion sensors and improved signal processors for such systems.

BACKGROUND ART

This invention is particularly useful for the antitheft protection of motor vehicle, construction equipment, and other high value apparatus in which a security system can be housed. While not limited thereto the invention is particularly useful for the protection of apparatus which is normally moved from place to place or is fixed to an immovable structure. If the apparatus to be protected against theft cannot be made secure by enclosure or attachment, it is usual practice to attempt to sense the theft or attempted theft and, on that occasion, to initiate some preventive measure. A common preventative is to sound an alarm capable of attracting attention to the theft. The detection of motion is a logical choice when attempting to provide an apparatus which is applicable to the protection of a wide variety of portable apparatus in a multitude of different situations. However, designing a satisfactory motion sensitive security system is complicated by the need to differentiate between authorized and unauthorized movement. There is a need to provide operating power in a way that prevents defeat of the system and, in a truly universal system, there is a need to devise a sensor which is effective without regard to spacial orientation or temperature differences and other physical factors.

Prior systems have incorporated features to overcome these and other problems for particular applications. Arming switches, self contained power sources, time delay circuitry, and other means have been employed. In general, however, the inclusion of such features to solve a problem peculiar to one application has rendered the system less useful, or even useless, in other applications. The need remains for a sensor and a system which has wide application, and one purpose of the invention is to satisfy that need.

SUMMARY OF INVENTION

It is an object of this invention to provide an improved motion sensor suitable for sensing motions associated with theft of apparatus. Another object is to provide an improved motion signal processor for security systems. A further object is to provide a security system capable of being arranged to sense motion in intervals in which motion is not authorized and to ignore motion when motion is authorized, is operative without regard to spacial orientation of the sensor, which can be made responsive selectively to motion in any direction, or to a specific motion, which can be used in either a permanent or temporary installation mode, and which has other features directed toward universality.

These and other objects and advantages of the invention which will be made apparent in the description that follows are realized, in part, because of the improved

sensor of the invention and, in part, because of its improved signal processor. In preferred form, the sensor comprises a coil adjacent to which a magnet is suspended such that the magnet is freely moved toward and away from the coil, from side to side of the coil in a plane over the coil, and rotationally on an axis which lies in a plane parallel to the coil. The suspension element is a resilient member lying, when relaxed, in a plane parallel to the plane of the coil windings, and, in the preferred form, substantially in the plane containing the center of gravity of the magnet and its mounting structure.

The coil is part of the signal processor. Signals induced in the coil are applied to a band pass amplifier, in the preferred embodiment, whose output is compared in a comparator to a selected standard. Provision is made for altering the standard with a signal such, for example, as might be applied by a switch sensitive to the state of some condition. The comparator output is integrated and is made, at a selected, accumulated signal value, to make energy available for signalling that unauthorized motion has been detected. A timing means terminates the unauthorized motion signal some predetermined time after the integrated signal level falls below a threshold value. Another timer delays integrator operation for a selected time following activation of the system.

The interaction between the several timing circuits, four in the preferred embodiment, is special as is the relation between the timing system and the sensor.

A means is included in the invention for rendering this system inactive for a selected time primarily to avoid sensing motion as an incident to activating the system. In the preferred form that means is proximity sensitive and unauthorized motion is announced by an audible alarm. To make it convenient and effective to use an automotive horn as the sounder, the signal processor includes a means for interrupting horn operation at a frequency in the audible range or below.

The "motion" detecting means in one preferred form of the invention is capable of sensing either or both of acceleration or jerk. Also, that preferred form employs simplified circuitry for arming and disarming the system.

BRIEF DESCRIPTION OF THE DRAWINGS

In the drawings:

FIG. 1 is a perspective view of a system which incorporates the preferred form of the invention;

FIG. 2 is a circuit diagram of the sensor and signal processing section of the system of FIG. 1;

FIG. 3 is a cross-sectional view, partly schematic, of the sensing and signal processing unit of the system taken on the vertical center plane of the unit;

FIG. 4 is a cross-sectional view of the sensor section of the sensor and signal processing unit taken on line 4-4 of FIG. 3;

FIG. 5 is a cross-sectional view taken on line 5-5 of FIG. 3; and

FIG. 6 is a diagram showing a portion of the circuit of FIG. 2 in an alternate, preferred form.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The system shown in FIG. 1 of the drawing is generally designated 10. It includes an inclosure 12 which houses a sensor and signal processing electronics and is

called the "sensing and signal processing unit." In addition, the system comprises a wiring harness generally designated 16. It extends from the unit 12 and includes connector terminals 18 and 19 for connection to a battery or other source of electrical power. The harness also includes two multiple connector jacks. One of those jacks is numbered 20 and it is interconnected with the plug 21 of a cable 22 that extends to the speaker unit 14. Two plugs are fitted into the other jack 23. One of those plugs is connected by a cable 24 to a spring opened plunger operated switch 25 in parallel with a condition sensor 125. The other plug is connected by a cable 26 to a reed switch 27.

The preferred embodiment includes these several connectors and jacks and plugs so that the system may be readily reconfigured for different applications. If the system is to be permanently installed in an automobile it may be preferred to omit the loud speaker unit 14 and to use the automobile's horn instead. In addition, it may be preferred to omit the battery that is housed in enclosure 12 and instead derive power from the automobile's battery through terminals 18 and 19. The primary sensor utilizes a resilient member and mass combination but, in some cases, particularly in cases of automobiles, it may be desirable to use a mechanically acutated switch to detect some kinds of unauthorized action such, for example, as opening of the automobile's hood or of the automobile's door. That kind of unauthorized action is readily sensed by the plunger switch 25, but a switch of that kind may be unnecessary, and would be omitted, in other situations such, for example, as when the system is attached temporarily to a piece of road building equipment which is to be left on the job site overnight. For an application of that kind it is more convenient to use the internal battery as the power source rather than to attempt to connect the system to the power source of the system of the unit to be protected. Also, in that application the use of the plunger operated motion sensor may be undesirable.

In some applications it is desirable to provide a means for disarming the system at a position known only to the authorized person or persons. In some applications of the system the inclusion of such a switch is desirable. In other applications it might not be needed.

The primary sensor and the signal processing circuitry are packaged so that they can be mounted together at any convenient place within the apparatus to be protected. The sensor responds to acceleration and it is arranged so that it will respond to acceleration in any direction. The sensing apparatus is constructed so that it will sense any acceleration from a very low value to a very large value. The sensitivity of the system is controlled in the signal processing unit and is adjustable to fit the practical circumstance surrounding the application of the system.

Not only will the sensor sense motion in any direction but its response to acceleration is relatively independent of the spacial orientation of the unit 12. That feature is particularly important when the system is moved from one security test to another. Even when it is not as, for example, when permanently mounted in a motor vehicle, the fact that the sensor is omnidirectional permits a wider choice of mounting arrangements.

The preferred form of sensor employs a mass resilient member spring arrangement in which movement of the mass causes movement of a magnet in proximity to a pick-up coil. The coil is located in the field of the magnet which ordinarily forms at least part of the mass so

that a voltage is induced in the coil as a consequence of movement of the mass. The value of the mass and the stiffness of the resilient member are selected so that the magnet will be moved in significant degree in response to even very small values of motion. A popular term for such an apparatus is "motion detector." In FIG. 2 the magnet is identified with the reference numeral 30, and the coil is numbered 31.

Signal Processing Circuit

The signal processor of preferred form employs integrated circuit devices that require energization from sources that are both more positive and more negative than intermediate or reference potential. That requirement is met by the power supply circuitry shown in the lower left corner of FIG. 2. The power supply, which is generally designated 32, includes terminals 18 and 19. They are arranged for connection through a main power switch to an external battery the positive side of which is connected to terminal 18 and the negative side of which is connected to terminal 19. Terminal 19 is connected by line 33 to system ground identified by the symbol marked 34. The positive terminal 18 is connected by line 35 to a supply terminal W and to a rectifier 36 the other side of which is connected by line 37 to the positive terminal 38 of the signal processor circuitry. The internal power source is a battery 40 which is connected in series with a switch 41 between lines 35 and 33. Transients in this system are filtered out by a capacitor 42 which is connected between lines 37 and 33. Resistors 43, 44 and 45 are connected in series, in that order, between line 37 and line 33. A power terminal Y is connected to the juncture of resistors 43 and 44, and a power terminal Z is connected to the junction between resistors 44 and 45. A second voltage divider is formed by resistors 46 and 47 which are connected in series, in that order, between lines 37 and 33. The juncture of resistors 46 and 47 is connected to the reference voltage terminal which is numbered 48.

Just above the power circuit 32 of FIG. 2 is an audio oscillator. It includes a comparator 50 whose output is connected by resistor 51 to its positive input and by resistor 52 to its negative input. The positive input of the comparator is connected to the junction of resistors 53 and 54 which are connected to form a voltage divider between the positive line and negative ground. That voltage divider circuit includes a switch 55 which is opened to disable the oscillator when, for example, the speaker or alarm device includes its own modulator or is not to be modulated.

The negative input of the comparator 50 is connected to the juncture of a resistor 56 and a capacitor 57 which are connected in series from the positive line to ground and together form the frequency control circuit of the oscillator.

The output of the comparator 50 is applied through the parallel combination of diode 58 and resistor 59 to the positive input of a comparator 60 and to the positive line through another resistor 159. A resistor 161 connects the output of the comparator with the positive input. The negative input is connected by a line 61 to a control circuit to be described below. The output of the comparator is also connected to the negative input of a comparator 62 whose positive terminal is connected to the reference line. The output of the latter is connected to the base of a transistor 64 through a resistor 65. The emitter of the transistor is connected to ground voltage and the collector is connected by resistors 66 and 67, in

series, to the positive line. The junction of resistor 66 and resistor 67 is connected to the base of a power transistor 68 whose emitter is connected to the power terminal W and whose collector is connected through the jack and plug set 20-21 to the output sounding device 74. A pair of diodes, one connected across the emitter and collector of transistor 68 and the other connected from its collector to circuit ground, protect the transistor.

The oscillator and amplifier are operative only when the output of comparator 80 is applied through the adjustable resistor 81 to line 61 to apply a positive signal to the negative input terminal of the comparator 60. A diode 82 is connected between line 61 and the positive terminal, and the capacitor 83 is connected between line 61 and circuit ground.

The negative input of comparator 80 is connected to the power terminal Z between resistors 44 and 45 of the power circuit 32. The positive input of comparator 80 is connected to line 84. A timing circuit formed by the parallel combination of a capacitor 85 and a resistor 86 are connected between line 84 and ground. Line 84 extends to a junction 87. That junction is connected to the collector of a transistor 88 whose emitter is connected to circuit ground and whose base is connected through a resistor 89 to the output of a comparator 90 whose positive terminal is connected to the power terminal Y between resistors 43 and 44 of the first described voltage divider network in power circuit 32. The negative terminal of comparator 90 is connected to the junction of resistor 91 and capacitor 92 which are connected in series, in that order, between the positive line and ground. The resistor and capacitor form a timing circuit. Provision is made for rendering that circuit inoperative by shorting the capacitor. The shorting circuit is formed in parallel with the capacitor and it includes the normally open reed switch 93 and the connector 23 of the wiring harness.

At the upper left in FIG. 2 coil 31 is disposed within the magnetic field of magnet 30. The coil is connected in series with a resistor 95 between the negative input terminal and the positive input terminal of an amplifier 96. The positive terminal of the circuit is connected to the reference potential line of the system, and a capacitor 97 is connected in parallel with the combination of coil 31 and resistor 95. The output of the amplifier 96 is connected by the parallel combination of a resistor 98 and a capacitor 99 to the negative input terminal of amplifier 96. In addition, the output of amplifier 96 is connected through a coupling capacitor 100 and a series resistor 101 to the negative input terminal of an amplifier 102 whose positive input is connected to the reference potential line. The output of amplifier 102 is connected by the series combination of a resistor 103 and a parallel circuit consisting of resistor 104 and capacitor 105 to the negative input terminal of the amplifier 102. The junction between the resistor 103 and the parallel circuit is connected by a resistor 106 to the reference potential line. In addition, the output of amplifier 102 is connected to one end of a series circuit formed by resistor 107 and capacitor 108 between the output of amplifier 102 and the reference potential line, in that order. The junction between resistor 107 and capacitor 108 is connected to the positive input terminal of amplifier 110 whose negative input terminal is connected to the output of that amplifier. The output is also connected through the series combination of a potentiometer 111 and a fixed resistor 112 to the positive line. The junction

between the potentiometer and the fixed resistor is connected through the jack and plug set 23 to one side of the normally open plunger switch 25 whose other side is connected to circuit ground. The tap of the potentiometer is connected to the negative input of another comparator 113 whose positive input terminal is connected by line 114 to the output of amplifier 102. The output of comparator 113 is connected through a diode 115 to the junction point 87.

Diode type 1N4001 may be used everywhere where a diode is indicated in the diagram. The several amplifiers and comparators in the circuit are integrated circuit type 324. Appropriate values for the other elements of the circuit are listed in the chart below.

Component Values

	Value
<u>Resistors</u>	
43, 45, 47, 89, 107, 112	27K ohms
44, 59, 101, 81	100K ohms
106	1K ohms
56, 104	1 Meg ohms
46, 51, 52, 53, 54, 67, 98,	
103, 111, 112	10K ohms
86, 91	470K ohms
<u>Capacitors</u>	
42, 97, 99, 105, 108	0.1 mfd
57, 83, 85, 92, 100	100 mfd

Operation of the Circuit

The sounder 74 is energized when transistor 68 is turned on. The horn circuit includes a make-and-break switch so that the horn will sound notwithstanding that it is energized from the unidirectional source. Transistor 68 is turned on by the output of current amplifier 62 when comparator 60 is rendered conductive. The comparator 60 is turned on when the voltage across capacitor 83, which is applied to the negative terminal of comparator 60 by line 61, exceeds the potential at the positive input of comparator 60. The potential at the positive terminal is established by the resistive network formed by resistors 56, 52, 59, 159 and 161, and the voltage that is applied to that network from the positive side of the power source, and the output of the comparator 50 which is connected as a multivibrator.

In summary, the sounder 74 will be turned on and off at a rate determined by the multivibrator when the potential across capacitor 83 exceeds some threshold value. Capacitor 83 is charged by comparator 80 through the variable resistor 81 at a rate that is determined by the output potential of the comparator and the value of the resistor. Comparator 80 is turned on to charge the capacitor 83 only when the potential at its positive input exceeds the reference potential Z which is applied to its negative input. The potential at the positive input is equal to the potential across capacitor 85. A discharge resistor 86 is connected in parallel with capacitor 85 to form a timing circuit. A means is incorporated in this system for preventing the accumulation of charge on capacitor 85, or for rapidly discharging the capacitor, and in this preferred embodiment that means comprises the transistor 88 whose collector/emitter circuit is connected in parallel with the capacitor. When that transistor is rendered conductive the capacitor is shorted to ground. Conduction is controlled by comparator 90 whose output is applied to the base of transis-

tor 88. The comparator has its positive input connected to a reference source of positive potential. The negative input is connected to a timing circuit formed by the series combination of resistor 91 and capacitor 92. The output of the comparator 90 will turn the transistor 88 on until the capacitor 92 charges through resistor 91 to a value that exceeds the potential at the positive input of the comparator. As a consequence of that, transistor 88 is turned on and the capacitor 85 is prevented from being charged for an interval following application of power to the circuit until the capacitor 92 has been charged. Closure of the reed switch 93 will discharge capacitor 92 and result in a turn on of comparator 90 to turn on the transistor 88 and prevent capacitor 85 from being charged until the switch 93 is reopened and the capacitor 92 has been charged through resistor 91.

Capacitor 85 is charged by output current from comparator 113 through diode 115 as an incident to detection of motion at coil 31. Motion of the magnet induces a voltage in coil 31 and that voltage is applied across the positive and negative inputs of amplifier 96. The output of amplifier 96 is applied to the input of amplifier 102. The function of the several resistors and capacitors that are associated with amplifiers 96 and 102 is to limit the frequency response of the system to values that correspond to the frequency of voltage variations induced in coil 31 for the kind of motion and acceleration to be detected. In practice, and in this preferred embodiment, the amplifier 102 will provide an output in response to changing input at frequencies below about ten kilohertz. For practical reasons, the circuit is made responsive to frequencies in the range between about eight cycles per second and 160 cycles per second. The output of amplifier 102 is applied directly to the positive input of comparator 113 and is applied to the negative input of that comparator through the combination of current amplifier 110 and a time delay circuit formed by resistor 107 and capacitor 108. Use of the delay circuit results in compensation for any offset in the output of amplifier 102. In the absence of motion the output of amplifier 102 does not change and equal potentials are applied to the inputs of comparator 113. When the output of amplifier 102 is changed the delay in applying the change to the negative terminal will result in input differences that turn on the comparator 113 and result in the charging of capacitor 85.

Summarizing the operation of the system, acceleration is detected by the combination of magnet 30 and coil 31, and results in the charging of capacitor 85. That capacitor having been charged, comparator 80 will apply an output through resistor 81 to capacitor 83. After some time interval, the duration of which can be adjusted by adjustment of the value of resistor 81, capacitor 83 will be charged above a threshold value and will result in comparator 60 and the horn 74 being turned on.

There are applications for the system in which it is desired that the alarm be sounded in response to activity that is most easily sensed with a switch, current sensor or a sensor of some other condition related to a violation of security. Thus, for example, it may be desirable to sound the alarm if the vehicle door or hood or trunk lid is opened whether or not that motion is sensed by the acceleration sensor. The preferred system includes such a switch, numbered 25 in FIG. 1 and connected between ground and the junction between resistors 111 and 112 in FIG. 2. If switch 25 is closed the output of comparator 113 will go high. Capacitor 85, and thus

capacitor 83, will become charged and the horn will operate as previously described. A condition sensor 125 in this case a circuit whose output goes low when ignition current flows, is connected in parallel with switch 25.

The system is enabled or disabled by interrupting the power source. The means for interrupting energy from an external power source is not shown in the diagram. The switch 41 is used for interrupting energy supply when the source is internal. When the sensing and signal processing unit is mounted in a relatively inaccessible place the switch 41 would be mounted at a place more conveniently accessible.

There are two ways to disable the unit. One is to open the power supply circuit, and the other is to close the reed switch 93. In preferred form the reed switch is magnetically actuated and is used when it is desired to disable the system for a short period of time. The system is disabled immediately when the switch 93 is closed because closure discharges capacitor 92 and results in the immediate discharge of capacitor 85. Resetting is delayed until capacitor 92 is recharged above the threshold level through resistor 91. The time that the horn continues to be activated following the cessation of motion is determined primarily by the discharge rate of capacitor 85, and that is determined by the combination of the amount of its capacitance and the resistance of resistor 86.

The interrelationship of the several timing circuits to one another and to the motion detector is special. The motion detector has a natural oscillation frequency in each of its several movement modes which lies within the passband of the circuit between coil 31 and capacitor 85. Acceleration or other motion once detected results in oscillation of the magnet (or coil if it is the coil that is resiliently mounted) to provide a signal which continues for some period even if acceleration is limited to a very short interval.

Capacitor 85 of the third timing circuit is charged rapidly once the comparator 113 begins conducting current but only if transistor 88 is turned off. The transistor serves as a short circuit around capacitor 85 until capacitor 92 of the first timing circuit is charged. It begins charging when the system is powered and it charges slowly through resistor 91. Thus, while the sensor and its circuitry are immediately available to charge capacitor 85, charging is delayed to permit powering and enabling the system without sounding the alarm.

While it is charged rapidly from comparator 113, capacitor 85 discharges slowly through resistor 86. As a consequence comparator 80 supplies charging current to capacitor 83 of the second timing circuit over a relatively long period. Capacitor 83 discharges through a different circuit over a longer period. That arrangement of timing circuits insures that system operation is substantially the same in response to actuation of the specific motion detection switch 25 as to acceleration of magnet 30. It permits setting alarm time at resistor 81 independently of system sensitivity which is set at resistor 111, and it delays turn off if the alarm is on when the switch 93 is closed. That latter feature is important because the thief who has set off the alarm and finds switch 93 in his attempt to silence the alarm cannot tell by its actuation that he has found the disabling switch.

The Motion Detector

The motion or acceleration detector is formed by the combination of a magnet and a coil arranged so that relative motion between them results in induction of a potential in the coil. In the preferred embodiment the coil 31 is fixed and the magnet 30 is suspended over it by an elongated resilient member which extends in a plane perpendicular to the plane containing the coil and magnet. In the preferred form the magnet is made cylindrical and is mounted so that the axis of the cylinder is substantially coincident with the axis of the coil. The coil is round and its inside diameter is greater than the diameter of the cylinder. The magnet is suspended so that the magnet face toward the coil does not extend into the coil, and it is mounted in the enclosure so that a majority of the flux lines extending from one end of the magnet to the other are confined within the enclosure and will be unaffected by magnetic structure which are external to the housing such, for example, as magnetic structures on which the housing might be mounted. That arrangement ensures that a substantial number of flux lines will be cut by the pick-up coil 31 as an incident to even small motion of the magnet in any direction. As a consequence, a voltage will be developed in the pick-up coil if the magnet is moved in the direction of its axis toward or away from the coil. A voltage will be generated in the pick-up coil if the magnet is moved so that its axis is displaced in any direction from the axis of the coil, and a voltage will be generated in the coil if the magnet is moved so that its axis is tilted with respect to the axis of the coil. The magnet is suspended by a resilient member in a way that ensures that a number of these possible motions will occur in the event that there is any movement of the magnet relative to the coil. As best shown in FIGS. 4 and 5, the magnet in the preferred embodiment is mounted at a mid-region along the length of an elastic cord which is stretched across the sensor cavity of the housing its ends held in place by clamps which are integrally formed with the housing.

The enclosure 12 is divided into two compartments. One is designated 200 and is the compartment which contains the signal processing electronics and, in some versions of the preferred embodiment, the horn and the power supply battery. The other compartment is identified by the reference numeral 202 and it is the one that contains the sensor. The lower wall of the sensor compartment 202 is numbered 204. Conformations on the inner side of that lower wall define an annular inwardly projecting wall 206 whose axis is perpendicular to the plane of the wall 204.

The coil 31 surrounds that annular wall. Two ribs 210 and 212, respectively, extend across the sensor cavity one on each side of coil 31. Those ribs are integrally formed on the inner surface of the bottom wall.

Together those several conformations protect the coil against being struck by the magnet structure and damp excessive movement of the magnet without limiting the generation of signal voltages.

In this preferred embodiment magnet 30 is lodged in a cylindrical cup 214 which embraces the magnet except at one face, the lower face in FIGS. 3 and 5. The cup 214 is integrally formed with the suspension members which extend from diametric points on the cup wall substantially in the plane of the center of gravity of the magnet and cup assembly. The suspension members are numbered 216 and 218, respectively. They are sub-

stantially alike in length and in diameter and in every other characteristic, and each terminates in an enlargement or keeper which, in this form, is substantially cylindrical. The cylindrical end of the arm 216 is numbered 220, and the cylindrical end of the arm 218 is numbered 222. Each arm, adjacent its respective cylindrical end, resides in a notch formed in the upper face of a crossmember that extends across the interior of the sensor section of the housing parallel to the ribs 210 and 212. The rib associated with arm 216 is numbered 224 and the rib associated with arm 218 is numbered 226. Fingers formed on the inner wall of the cover 230 extend downwardly toward ribs 224 and 226, respectively. The finger 232 extends down into engagement with the upper surface of rib 224 on the opposite sides of the notch in which arm 216 is disposed, and at the other side finger 234 extends down and engages the upper surface of rib 226 on opposite sides of the notch in which arm 218 is disposed. In this preferred embodiment each of the arms is twisted three turns each in opposite directions at the time of assembly. The arms are held in place in notches so that they do not become untwisted in the assembly process.

The dimensions of the resilient arms and the weight of the magnet are not critical. However, the natural resonant frequency of the mass and resilient member combination should lie in passband of the signal processor, in this particular case between ten and 150 cycles per second in any orientation of the housing. Beyond that it is only required that the magnet remain suspended in any orientation so that it is free to move from side to side and to rotate about the axis of the arms and to move in the direction of the axis of the coil.

Alternative Signal Processing Unit

Large trucks are attractive objects for thieves not only because of the value of the truck but especially because of the value of their cargos. Protecting them is more difficult than protecting smaller vehicles because many truck designs afford easier access to the engine compartment and electrical system, especially from below. Certain features of the invention, while having general application, are especially useful in the case of large trucks. One of those features is the ability to detect heavy, short time application of forces by detecting jerk as distinguished from acceleration. Forces resulting in acceleration of portions of a vehicle occur in normal use so it is necessary to incorporate delays in security apparatus to permit deactivation of the system for normal use. Those time delays present opportunity for thieves who understand the construction and operation of the system. But long time delays are not required in the case of jerk, and response to jerk removes the possibility of disabling the security system with sharp, impacting blows.

Other improvements and functions are provided in the preferred form of the invention for certain applications. Some of them relate to alternative means for developing input signals to which the system is to respond, and one relates to an alternative arrangement for disabling the system.

The circuit of FIG. 6 illustrates how these added functions and features are achieved by modification of FIG. 2. Only so much of FIG. 2 is incorporated in FIG. 6 as is deemed necessary to illustrate where the changes and additions are to be made in FIG. 2. Reference numerals below 200 in FIG. 6 identify elements found in

FIG. 2. Added elements are identified by reference numerals greater than 300.

In FIG. 2 differential amplifiers 102 and 110 detect motion by measuring a function of acceleration which continues for a period which is compared to the timing circuit formed primarily by resistor 107 and capacitor 108, and has an amplitude which is compared to the voltage level set by potentiometer 111. The acceleration measuring elements of FIG. 6 are the same except that the input connections to the amplitude measuring comparator are reversed. Amplifier 302 of FIG. 6 is like comparator 113 of FIG. 2 except for reversal of input connections. Reversal of the comparator connections requires a change in reference potential because the polarity of the output to diode 115 and junction 87 is to remain the same. The change is accomplished by adjusting potentiometer 111 to change the polarity of the relative difference between input terminals without significant change in the magnitude of difference.

Reversal of comparator inputs simplifies the application of inputs from other external condition sensors. The condition sensor 125 and switch 24 and connector 23, all of which are found in FIG. 2, are replaced in FIG. 6 by transistors 306 and 308, current limiting resistors 310, 312 and 314 and a circuit interconnector 316. One side of the latter is connected to line 114 and the negative input of comparator 302. The other side of the circuit connector is connected to the collector of a transistor 306 whose emitter connects to positive d.c. power potential. The base of PNP transistor 306 is connected through resistor 310 to negative initiating signal line 318. A resistor 312 is connected between line 318 and positive d.c. power potential. The NPN transistor 308 has its emitter connected to the negative side of the d.c. supply and its collector connected to line 318.

In the absence of a negative potential on line 318 or of a positive potential at the base of transistor 308, the base of transistor 306 is positive because there is minimal voltage drop across the resistors 312 and 310. In that case, transistor 306 is turned off and no unbalancing potential is applied by transistor 306 to line 114 and comparator 302. However, if line 114 is made negative by a sensor or switch or the like, either directly or indirectly by turning on transistor 308 with a positive potential at its base, the transistor 306 will be turned on to unbalance comparator 302 and apply a signal to junction point 87. The response of the apparatus to such a signal has already been explained in the description of FIG. 2.

In FIG. 2 the combination of resistor 91 and capacitor 92 acting through comparator 90 and NPN transistor 88 delays enablement of the alarm system for a short time after opening of the reed switch 93.

Using a magnet which is carried on a key ring, a vehicle driver may close the hidden reed switch to discharge capacitor 92 whereby the alarm system is disabled until the capacitor is recharged. In FIG. 6 that portion of the circuit is modified to utilize a set of contacts which form a switch 320, as part of the ignition switch unit, to short circuit the capacitor 92 whenever the vehicle ignition switch is in the "on" position. A diode 342 and a limiting or timing resistor 344 have been added in series with the reed switch 93. The circuit of FIG. 6 assumes that potential at the ignition switch is positive, which is almost universal. That potential is applied by switch 320 to the base of NPN transistor 322 through a limiting resistor 324. The transistor's emitter is connected to system negative as is one side of capaci-

tor 92. The transistor's collector is connected to the other side of the capacitor. The voltage levels at which system activation is achieved is altered to accommodate the transistor characteristics by adding a comparator 326 between the junction of resistor 91 and capacitor 92 on one side and the negative input of comparator 90 on the other. The input terminals of comparator 326 are reversed so the junction between timing resistor 91 and capacitor 92 is connected to the comparator's positive input.

In certain cases it is desirable to have the security system provide an output to a sounder or otherwise in response to impact, or more accurately, jerk, in addition to the response occasioned by acceleration. To accomplish that result the form of the invention depicted in FIG. 6 includes still another integrator or timer coupled to still another amplitude comparator 328. FIG. 6 includes a resistor 330 and a capacitor 332 connected in series in that order from line 114 at the output of comparator 102 to the neutral point of the power supply. The junction between resistor 330 and capacitor 332 connects to the positive input of a comparator whose other input is connected to its output. That output is connected to one end of potentiometer 334. The circuit extends from the output of comparator 328 through the potentiometer resistor 334 and a dropping resistor 336 to the negative side of the d.c. power supply. The potentiometer slider connects to the positive terminal of a comparator 338 whose negative terminal connects to line 114 at the output of comparator 102. The output of comparator 338 is connected through a diode 340 to junction point 87 of FIGS. 2 and 6.

Thus the circuit formed by elements 330, 332, 328, 334, 336, 338 and 340 has the same configuration and is in parallel with the circuit formed by elements 107, 108, 110, 111, 112, 302 and 115. One provides an output in response to relatively low magnitude acceleration which continues for a relatively long period. The other provides an output in response to relatively high magnitude jerk which continues for a much shorter time. The difference in amplitude response is adjusted by relative adjustment of the potentials at the respective positive terminals of comparators 302 and 338 and that is done by adjustment of potentiometer settings. Measurement of duration is accomplished in resistor and capacitor 107 and 108 in the case of acceleration measurement. In one case resistor 107 has the value 1.0 megohm and capacitor 108, 0.1 mfd. In the jerk circuit, resistor 330 is only 220 K ohms and capacitor 332, 0.1 mfd.

Although we have shown and described certain specific embodiments of our invention, we are fully aware that many modifications thereof are possible. Our invention, therefore, is not to be restricted except insofar as is necessitated by the prior art.

We claim:

1. In a security system:

a motion sensor comprising a magnet and a coil disposed in the field of the magnet, one of the magnet and coil being fixed and the other being moveable relative to the fixed one in the direction toward and away therefrom in a first plane, and being moveable relative to the fixed one in a perpendicular plane perpendicular to said first plane and parallel to the plane containing said fixed one, and being moveable rotatably about an axis extending substantially along the intersection of said first plane and said perpendicular plane.

2. The invention defined in claim 1 which further comprises a signal processing means for sensing voltage variations across said coil and for providing an output signal incident to relative movement of said coil and magnet and for providing an output signal.

3. The invention defined in claim 2 in which said signal processing means includes a delay means effective to prevent provision of said output signal for a time following application of power to said system as a function of time.

4. The invention defined in claim 3 in which said signal processing means further comprises second time delay means effective to prevent provision of said output signal for a period following the sensing of motion by said motion sensor which period is independent of the magnitude of the sensed acceleration for magnitudes greater than a given magnitude.

5. The invention defined in claim 4 in which said signal processing means further comprises a third time delay means effective to continue provision of said output signal, once provided, for not less than a predetermined time period.

6. The invention defined in claim 4 in which each of said time delay means comprises a resistor and capacitor combination and in which the charge on the capacitor is changed;

the charge on the capacitor of the second being changed rapidly, provided that the charge on the capacitor of the third timing means is within a predetermined range of charges, upon the sensing of acceleration and returned toward initial value less rapidly.

7. The invention defined in claim 6 in which the charge on the capacitor of the second time delay means is changed in response to sensing of acceleration only during the interval when the charge on the capacitor of said first time delay means is returned toward its charged value.

8. The invention defined in claim 7 which comprises disabling means discharging the capacitor of the third timing circuit.

9. The invention defined in claim 2 in which said signal processing means comprises a comparator having a pair of input terminals each subjected to respectively associated signals as an incident to voltage variation across said coil, the signal applied to one of said input terminals being delayed relative to the time of application to the other input terminal of its associated signal.

10. The invention defined in claim 9 in which said magnet is suspended in the mid-region along the length of a resilient cord.

11. The invention defined in claim 10 in which said resilient cord comprises a pair of arms extending in opposite directions from said magnet, prestressed in torsion and in tension and each arm being fixed relative to said coil at a respectively associated point.

12. The invention defined in claim 1 in which said magnet is suspended in the mid-region along the length of a resilient cord.

13. The invention defined in claim 12 in which said resilient cord comprises a pair of arms extending in opposite directions from said magnet, prestressed in torsion and each arm being fixed relative to said coil at a respectively associated point.

14. The invention defined in claim 13 in which said coil is generally circular and lies, in a plane parallel to a plane containing said arms;

the magnet being mounted for movement along the axis of the coil exteriorly of the coil.

15. In a security system:

sensing means for providing a motion signal in response to motion imparted to an element of the sensing means;

a signal processing means responsive to said motion signal for providing an output signal;

said signal processing means comprising first, second and third time delay circuits the first time delay circuit being connected to delay operation of the second and third time delay circuits and the second time delay circuit being connected to delay provision of said output signal following receipt by said signal processing means of a motion signal for a period determined only by said second time delay circuit;

said third time delay circuit being connected to continue furnishing of said output signal following termination of the motion signal for a period determined, after completion of the operation of said second time delay circuit, only by said third time delay circuit.

16. The invention defined in claim 15 in which said signal processing means includes a sounder and means for applying said output signal to said sounder intermittently.

17. The invention defined in claim 16 in which said third time delay circuit comprises a third delay circuit capacitor connected to have its charge changed rapidly in response to a sensing signal and returned toward initial value more slowly following cessation of said sensing signal; and

in which said second time delay circuit comprises a second delay circuit capacitor whose charge is altered relatively slowly in intervals when the charge on said third delay circuit capacitor differs from initial value by more than a predetermined amount.

18. The invention defined in claim 17 in which the first time delay circuit comprises a first circuit capacitor connected to have its charge changed relatively slowly from an initial value upon the application of power to said signal processing means and connected to prevent alteration of the initial charge on said third circuit capacitor for a period following such application of power.

19. The invention defined in claim 18 which further comprises means in the form of a disabling switch connected to return the charge on said first circuit capacitor rapidly toward the value of charge on said capacitor prior to application of power to said signal processing means.

20. In a security system:

a magnet and a coil disposed in the field of the magnet such that a signal voltage is generated in the coil as an incident to relative movement between the magnet and the coil; and

a signal processor capable of sensing voltage variations across the coil and of providing an output signal, means for providing an output signal, said signal processor comprising first output signal providing means for providing an output signal in response to signal voltages greater than a first given magnitude for a period of first duration;

said processor further comprising second output signal providing means for providing an output signal in response to signal voltages greater than a second given magnitude for a period of second duration;

4,584,569

15

said first and second output signal providing means each comprising a time delay circuit and an associated comparator connected to compare the current amplitude of said signal voltage with its amplitude at a time prior by the amount of said delay.

21. The invention defined in claim 20 in which one of said first and second output signal providing means has a time delay circuit providing a relatively long delay and is arranged to provide an output signal in response to a voltage signal of some minimum amplitude, and in which the other of said first and second output signal

16

providing means has a time delay circuit providing a relatively short delay and is arranged to provide an output signal in response to a voltage signal having amplitude higher than said minimum amplitude.

22. The invention defined in claim 21 further comprises means for filtering from said signal voltage components which vary in amplitude at frequencies outside the range from eight to one hundred and sixty cycles per second.

* * * * *

15

20

25

30

35

40

45

50

55

60

65

REEXAMINATION CERTIFICATE (1309th)

United States Patent [19]

[11] B1 4,584,569

Lopez et al.

[45] Certificate Issued Jun. 19, 1990

[54] MOTION SENSITIVE SECURITY SYSTEM

[52] U.S. CL 340/566; 73/650;
73/654; 340/429; 340/571

[76] Inventors: Michael J. Lopez, 970 Calle Venado,
Anaheim, Calif. 92807; Howard A.
Williams, Jr., 2629 X. Griset Pl.,
Santa Ana, Calif. 92704; Henry J.
Salvatori, 10633 Virginia Ave.,
Whittier, Calif. 90603

[58] Field of Search 340/527, 528, 691, 384 E

[56] References Cited

U.S. PATENT DOCUMENTS

2,111,643 3/1938 Salvatori 310/25
3,158,831 11/1964 Boyer 310/329
3,197,756 7/1965 Maynard 73/517
3,995,268 11/1976 Ferrari 340/384 E
4,122,437 10/1978 Petersen 340/528
4,180,811 12/1979 Yoshimura et al. 340/566

Reexamination Request:

No. 90/001,806, Jul. 10, 1989

Primary Examiner—Glen R. Swann, III

Reexamination Certificate for:

Patent No.: 4,584,569
Issued: Apr. 22, 1986
Appl. No.: 650,835
Filed: Sep. 17, 1984

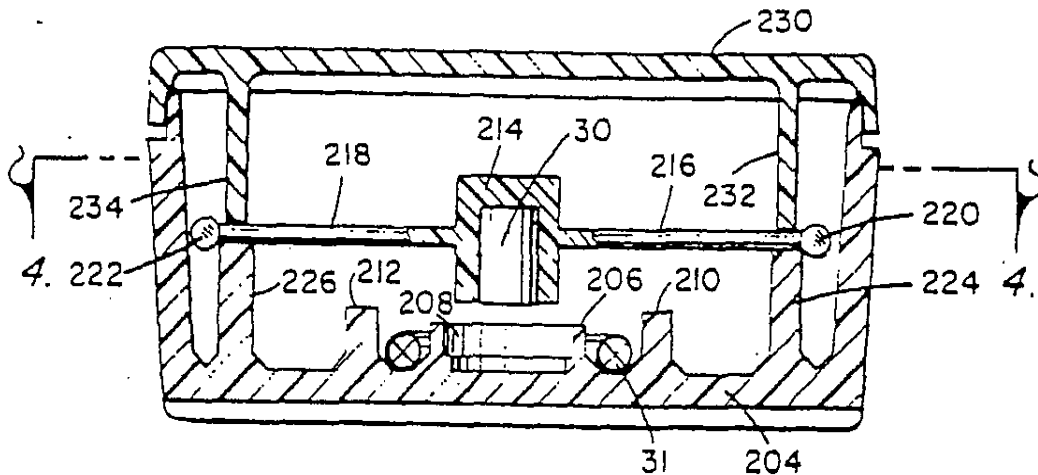
[57] ABSTRACT

The preferred arrangement utilizes a magnet suspended at the center of an elastic cord over a pickup coil. Movement of the magnet is sensed by the coil in that signals are generated by such movement. The signals are processed in the combination of a time delay circuit and a comparator to provide an output which is a measure of acceleration of the element on which the elastic cord is mounted and, in one form, by a measure of jerk in a similar time delay circuit and comparator combination.

Related U.S. Application Data

[63] Continuation-in-part of Ser. No. 324,170, Nov. 23, 1981, abandoned.

[51] Int. Cl.³ G08B 21/00



REEXAMINATION CERTIFICATE
ISSUED UNDER 35 U.S.C. 307

THE PATENT IS HEREBY AMENDED AS
INDICATED BELOW.

Matter enclosed in heavy brackets [] appeared in the patent, but has been deleted and is no longer a part of the patent; matter printed in italics indicates additions made to the patent.

AS A RESULT OF REEXAMINATION, IT HAS
BEEN DETERMINED THAT:

The patentability of claims 1-14 and 20-22 is confirmed.

Claim 15 is determined to be patentable as amended.

Claims 16-19, dependent on an amended claim, are determined to be patentable.

15. In a security system as defined by claim 1 wherein said motion sensor provides:

[sensing means for providing] a motion signal in response to motion imparted to [an element of the sensing means] said motion sensor;

a signal processing means responsive to said motion signal for providing an output signal;

said signal processing means comprising first, second and third time delay circuits the first time delay circuit being connected to delay operation of the second and third time delay circuits and the second time delay circuit being connected to delay provision of said output signal following receipt by said signal processing means of a motion signal for a period determined only by said second time delay circuit;

said third time delay circuit being connected to continue furnishing of said output signal following termination of the motion signal for a period determined, after completion of the operation of said third time delay circuit, only by said third time delay circuit.

* * * * *

25

30

35

40

45

50

55

60

65

US004584569B1

REEXAMINATION CERTIFICATE (3818th)

United States Patent [19]

[11] B1 4,584,569

Lopez et al.

[45] Certificate Issued Jul. 27, 1999

[54] MOTION SENSITIVE SECURITY SYSTEM 4,162,479 7/1979 Nickell et al. 340/528
 4,335,376 6/1982 Marquardt 340/528

[75] Inventors: Michael J. Lopez, Anaheim; Howard A. Williams, Jr., Santa Ana; Henry J. Salvatori, Whittier, all of Calif.

FOREIGN PATENT DOCUMENTS

2281609 3/1976 France
 1128733 10/1968 United Kingdom

[73] Assignee: Directed Electronics, Inc., Vista, Calif.

Reexamination Request:

No. 90/004,842, Nov. 21, 1997

Reexamination Certificate for:

Patent No.: 4,584,569
 Issued: Apr. 22, 1986
 Appl. No.: 06/650,835
 Filed: Sep. 17, 1984

OTHER PUBLICATIONS

Kurrelmeyer B. and Mais, W. H., Electricity and Magnetism, D. Van Nordstand Co., Inc., 1967.
 Richter, C. F., Elementary Seismology, W. H. Freedman and Company, 1968.
 Gurvich, I., Seismic Prospectin, MIR Publishers, 1972.
 Plonsey, R. and Collin, R. E., Principles and Applications of Electromagnetic Fields, McGraw-Hill Book Co., Inc., 1961.

Related U.S. Application Data

- [63] Continuation-in-part of application No. 06/324,170, Nov. 23, 1981, abandoned.
- [51] Int. Cl.⁶ G08B 21/00
- [52] U.S. Cl. 340/566; 73/650; 73/654; 340/429; 340/571
- [58] Field of Search 340/527, 528, 340/529, 530, 566, 429

Primary Examiner—Glen R. Swann, III

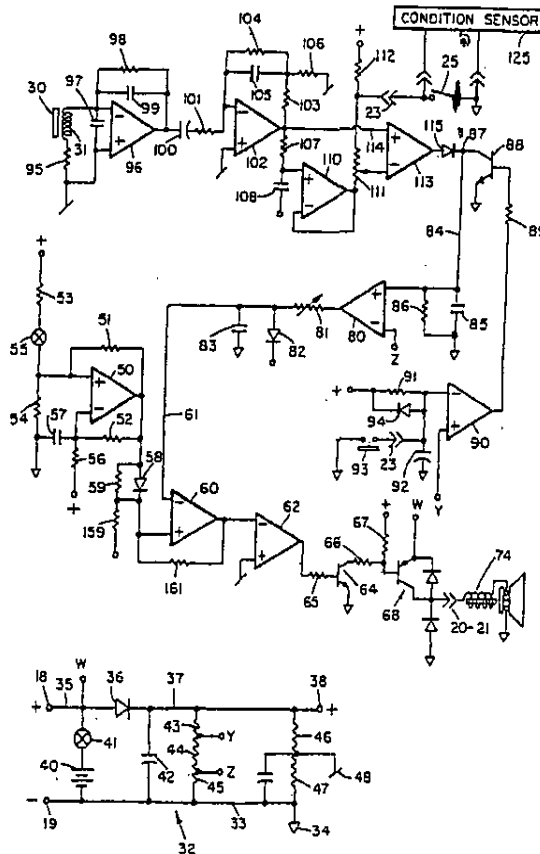
[57] ABSTRACT

The preferred arrangement utilizes a magnet suspended at the center of an elastic cord over a pickup coil. Movement of the magnet is sensed by the coil in that signals are generated by such movement. The signals are processed in the combination of a time delay circuit and a comparator to provide an output which is a measure of acceleration of the element on which the elastic cord is mounted and, in one form, by a measure of jerk in a similar time delay circuit and comparator combination.

References Cited

U.S. PATENT DOCUMENTS

2,659,065 11/1953 Cordell 340/690



B1 4,584,569

1

**REEXAMINATION CERTIFICATE
ISSUED UNDER 35 U.S.C. 307**

NO AMENDMENTS HAVE BEEN MADE TO
THE PATENT

2

AS A RESULT OF REEXAMINATION, IT HAS BEEN
DETERMINED THAT:

The patentability of claims 1-22 is confirmed.

* * * * *

United States Patent [19]

[11] Patent Number: **5,532,670**

Issa et al.

[45] Date of Patent: **Jul. 2, 1996**

[54] **METHOD OF INDICATING THE THREAT LEVEL OF AN INCOMING SHOCK TO AN ELECTRONICALLY SECURED VEHICLE AND APPARATUS THEREFORE**

4,866,417 9/1989 DeFino et al. 340/429
 5,084,697 1/1992 Hwang 340/566

Primary Examiner—Glen Swann
 Attorney, Agent, or Firm—Sam Talpalatsky

[75] Inventors: Darrell E. Issa, Vista; Jerry W. Birchfield, Escondido, both of Calif.

[57] **ABSTRACT**

[73] Assignee: Directed Electronics, Inc., Vista, Calif.

A method of indicating the threat level of an incoming shock to an electronically secured vehicle and eliminating spurious signals developed from the interaction of EMF and RF energy fields with the shock sensor including the steps of sensing a shock delivered to the vehicle indicative of an attempted intrusion, generating an electric signal the strength of which is proportional to the intensity of the shock, analyzing the signal to determine if it is of a low, generally non-threatening intensity or a higher, generally security-threatening intensity, ignoring the first 5 milliseconds of the signal produced by the shock sensor, ignoring all signals that do not disappear and later reappear, and producing either a first pulse representing a low intensity signal, or separate first and second pulses representing a signal containing both low intensity and higher intensity components.

[21] Appl. No.: 112,940

[22] Filed: Aug. 30, 1993

Related U.S. Application Data

[63] Continuation-in-part of Ser. No. 886,871, May 22, 1992, abandoned, and a continuation-in-part of Ser. No. 945,667, Sep. 16, 1992.

[51] Int. Cl.⁶ G08B 13/02

[52] U.S. Cl. 340/429; 340/566

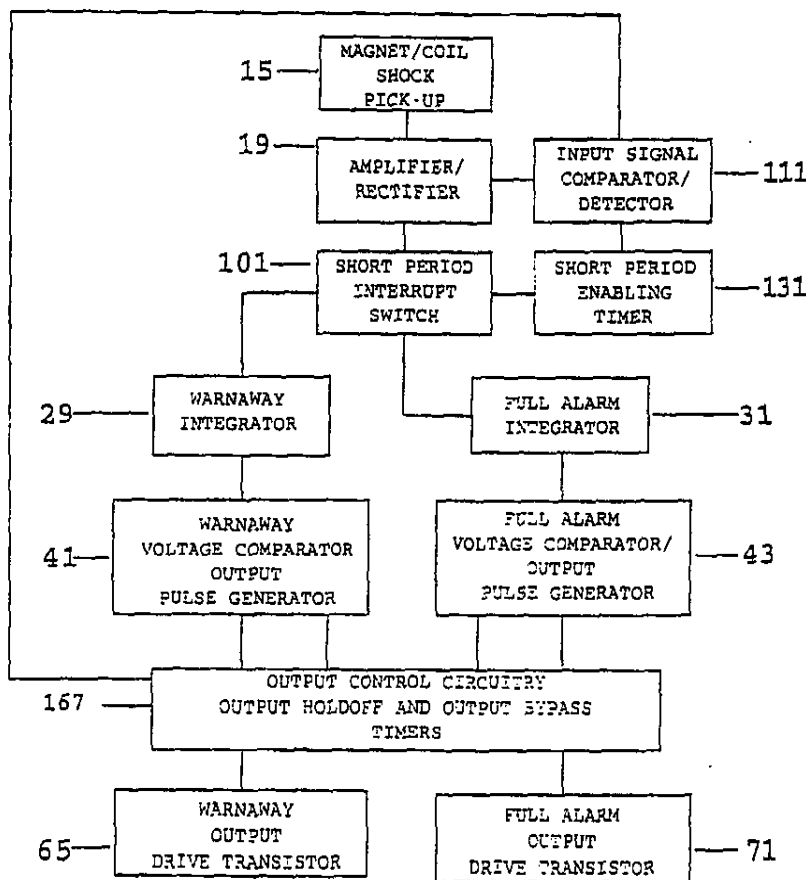
[58] Field of Search 340/429, 566

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,584,569 4/1986 Lopez et al. 340/429

40 Claims, 6 Drawing Sheets



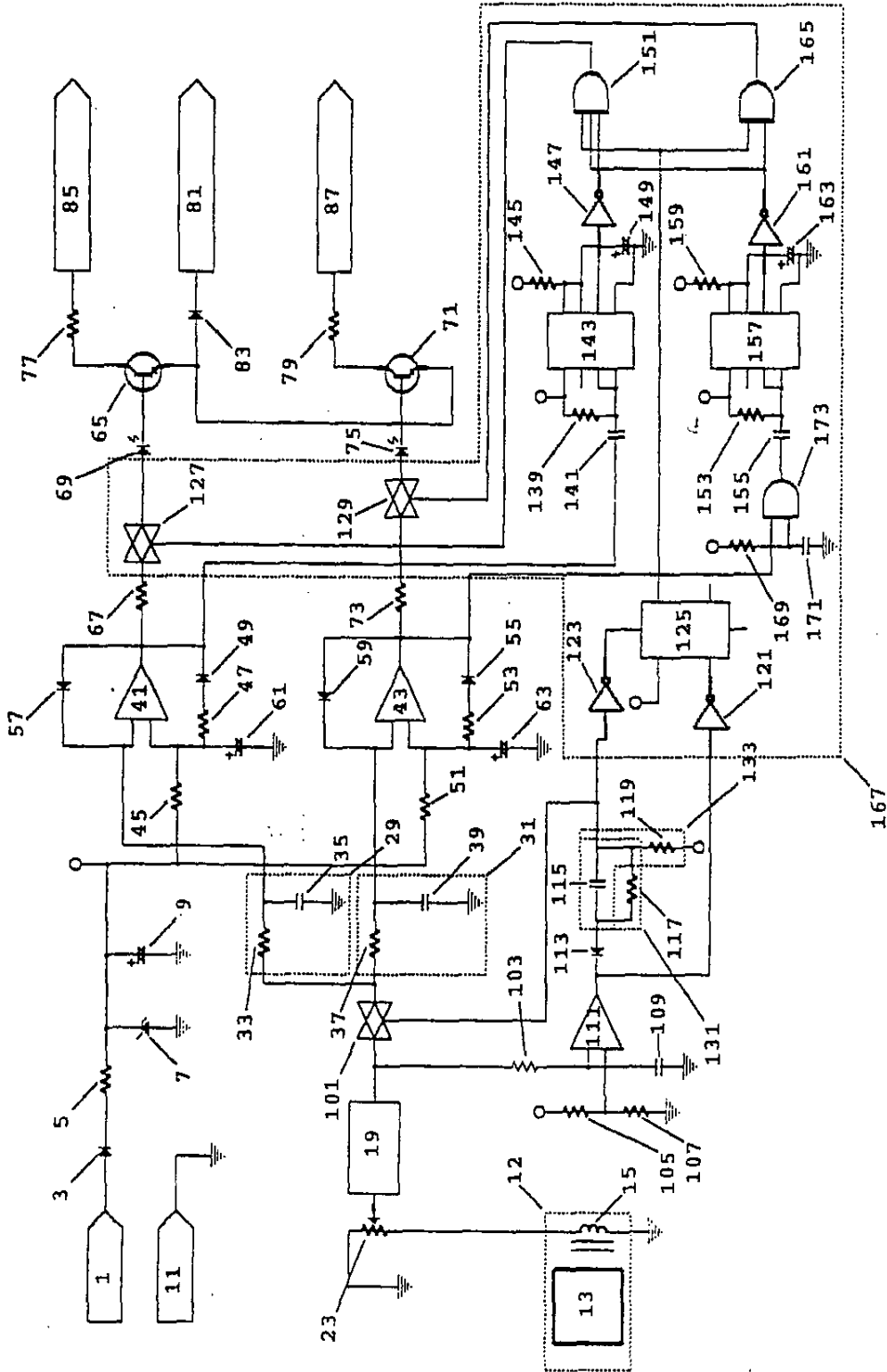


FIGURE 1

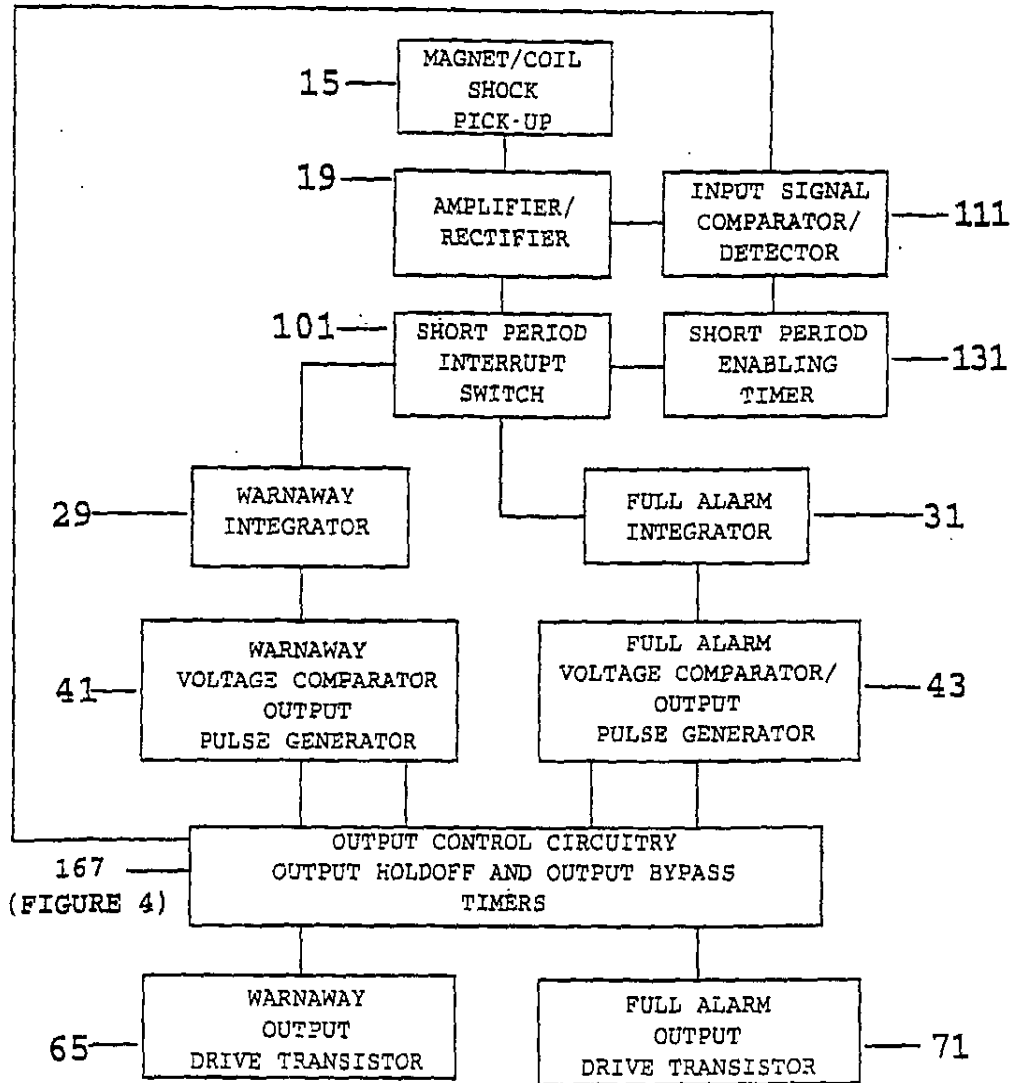


FIGURE 2

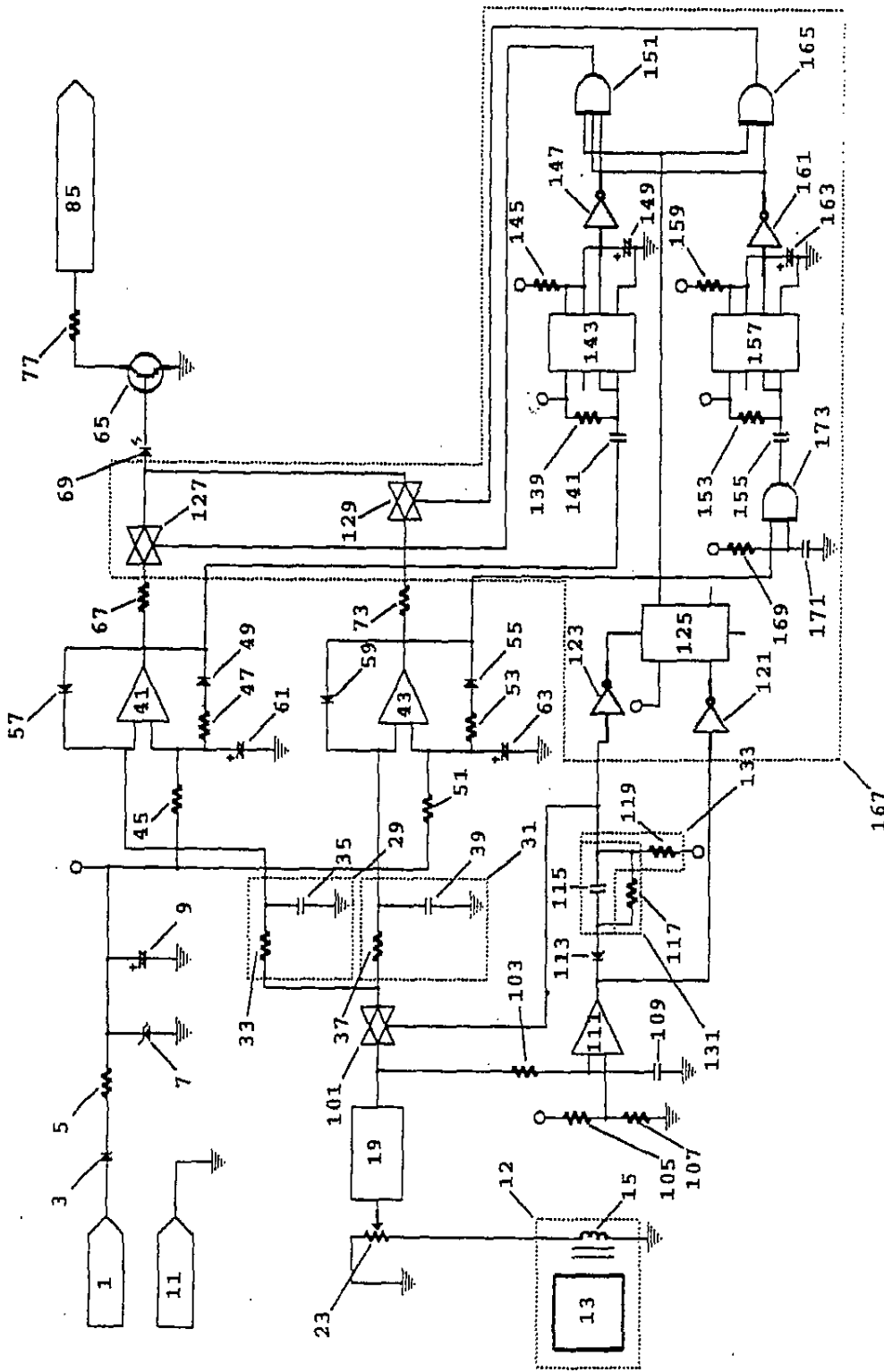


FIGURE 3

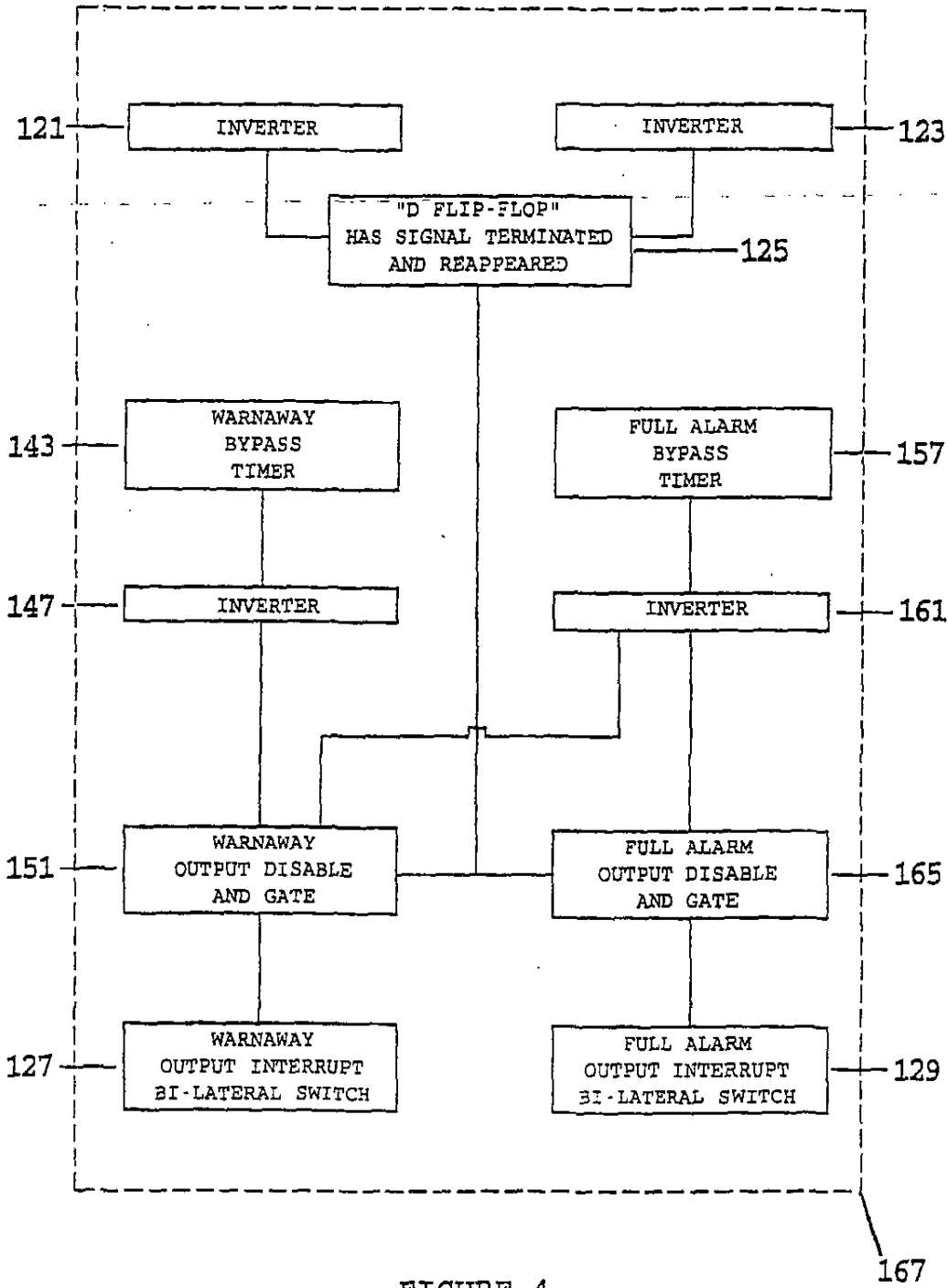


FIGURE 4

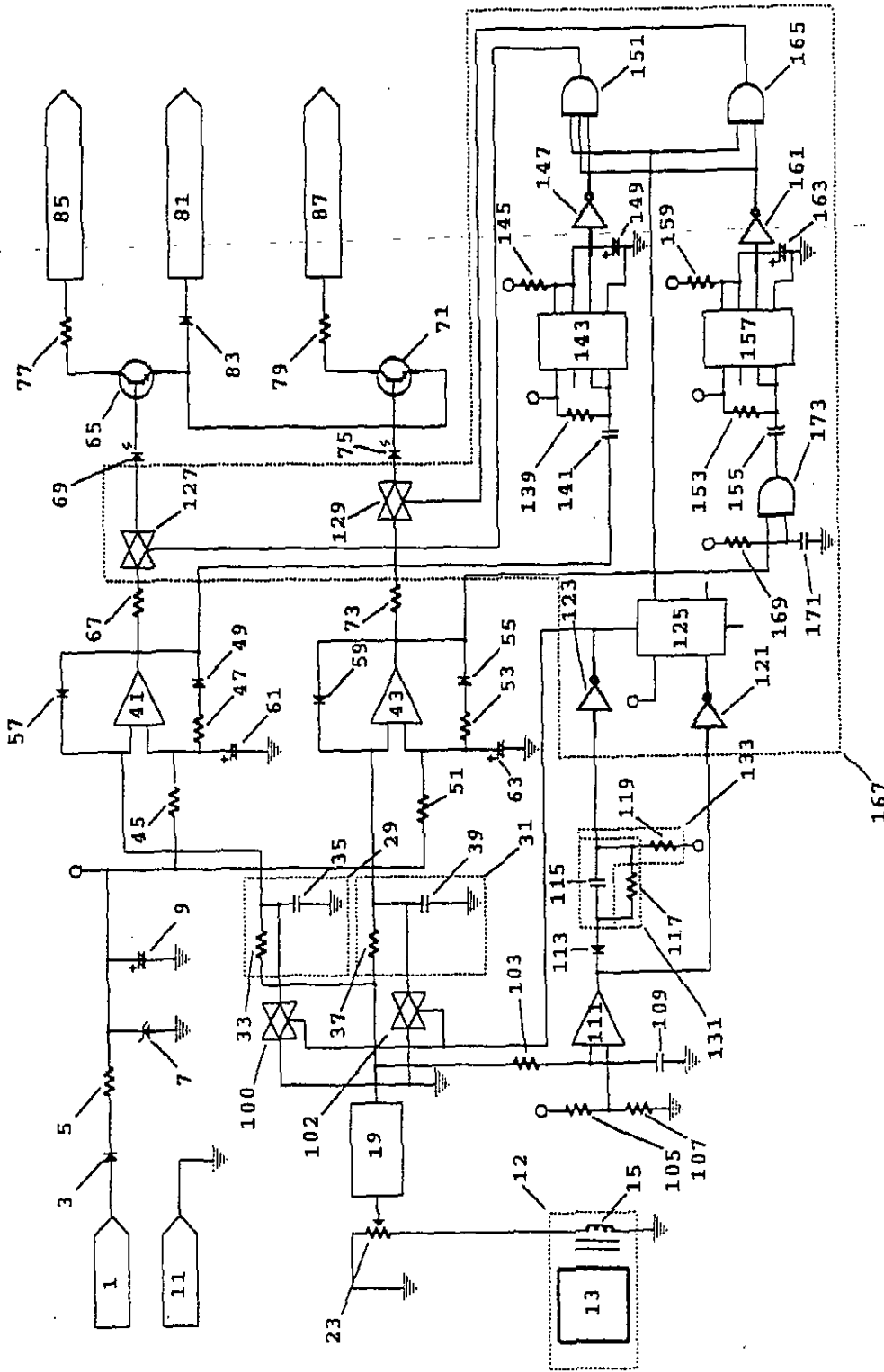


FIGURE 5

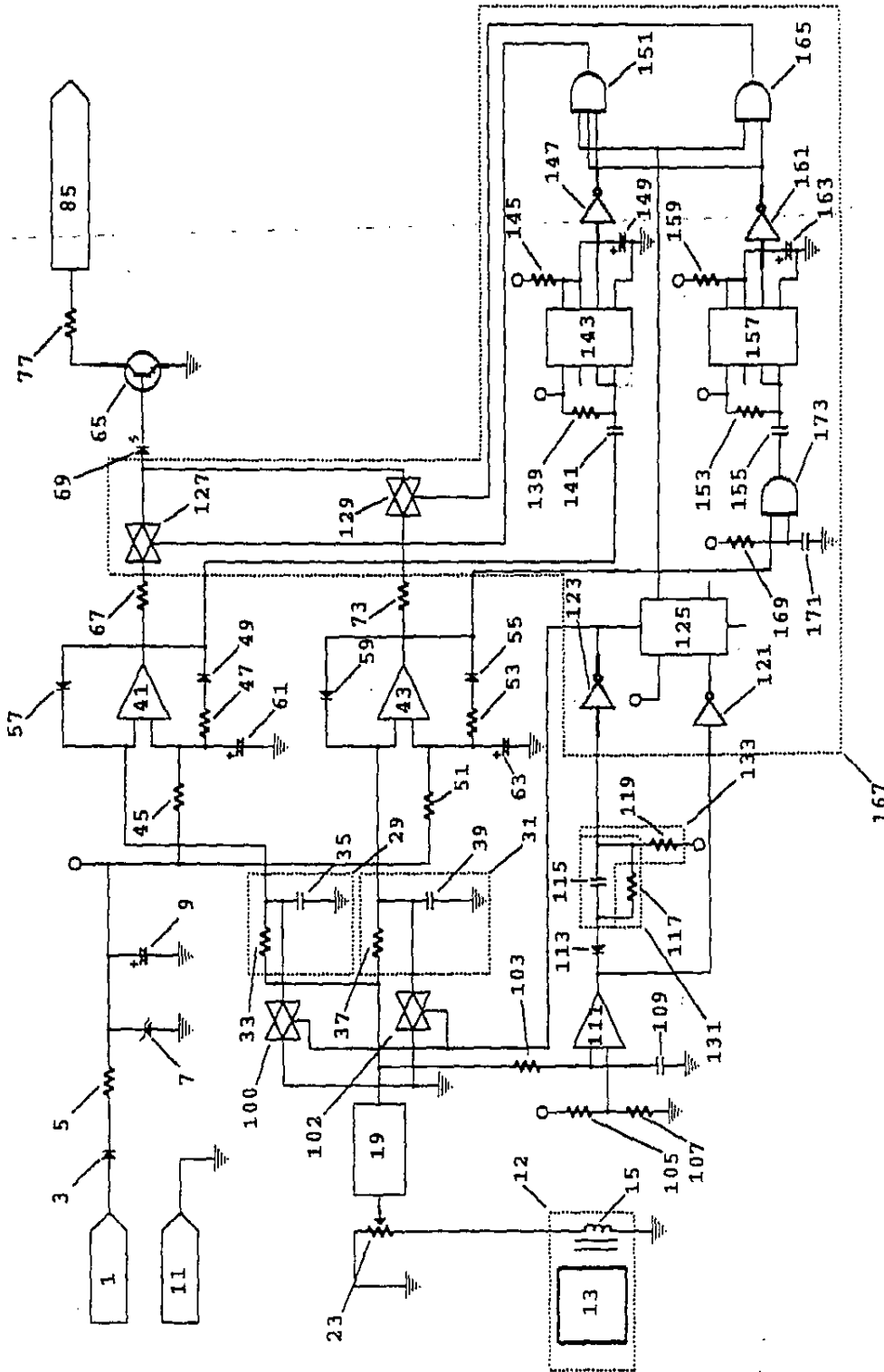


FIGURE 6

5,532,670

3

shocks delivered to the vehicle, using a single shock sensor of the type previously described. An alarm is produced that is proportionate to these shocks. The low intensity alarm is called a "warn-away" and is of a serious but far quieter nature and will generally get the proper message to the individual without engaging the full alarm. The person inducing the shock is quietly but firmly advised by prerecorded voice or a series of soft chirps of the limited intrusion while the vehicle owner is not required to attend the vehicle to shut off the alarm.

In addition, this invention includes the novel feature of providing full wave rectification of the output from the shock sensor and clipping or ignoring the first few milliseconds of the signal produced and further requires the signal to drop to its zero or reference voltage before triggering any warning alarm. Therefore, only physical assaults on the vehicle, as compared with "electrical" assaults, are allowed to proceed through the system to be subsequently analyzed and compared. These features therefore eliminate the spurious signals that are produced by non-physical assaults.

Most security systems involve only half-wave rectification of the induced signal emanating from the induction coil. Shocks to the protected vehicle may cause the detector, such as a magnet positioned adjacent the induction coil, to first swing away from the coil before swinging back toward the coil in periodic motion. In that situation, should the rectification include only the first swing away from the coil, the signal thereby generated would be of unnaturally low value and not be an accurate reproduction of the full intensity of the shock. Full wave rectification of the induced signal nullifies this anomaly and provides a signal representing a more accurate assessment of the shock. Therefore, the output from the magnet-induction coil is made more accurate and not so dependent upon whether the coil first moves toward the induction coil or away from it; a signal of similar strength is produced notwithstanding whether the magnet is first caused to approach the coil or recede from it.

The method and apparatus disclosed herein analyzes the signal produced by the changing magnetic field from the vibrating magnet and, in the case of a mild or low intensity shock, generates a pulse that may be used to activate a warn-away alarm that will automatically reset itself without intervention by the vehicle owner. The same method and apparatus will generate both the mild shock responsive pulse as well as a stronger second pulse when it is determined that the shock exceeds a specific energy level. Both the non-threatening and the threatening levels of incoming shock are constantly monitored by the apparatus.

When the non-threatening "warn-away" pulse is generated the threatening pulse generator is still in a monitoring mode and can be activated by a threatening level shock incoming to the vehicle even while a warn-away message is being given. If two or more mild shocks are received by the vehicle within a finite time period, such as 7 seconds, the system will produce a full alarm whereas if the mild shocks are repeated on a sequence longer in time than 7 seconds, a second and repeated "warn-away" alarm will be produced again.

The prior art has not yet appreciated these features and would continue to generate repeated "warn-away" alarms. In fact, in some cases the energy dispensed in the "warn-away" alarm is of sufficient magnitude to generate a low-threat level input that triggers another "warn-away" alarm so that the system continues to cycle "warn-away" alarms each induced by the preceding alarm.

Further, the invention herein contains the unique property of ignoring the first few milliseconds of signal produced by

4

the sensor. A physical shock lasts far longer and the energy level of the residual signal is sufficient to pass through an integrator to a comparator to determine the relative strengths of the shocks. The signals produced by RF bursts, EMF bursts and the like do not last beyond that period because there is no physical movement imparted to the magnet; the energy bursts only interacted with the induction coil. Accordingly, those signals produced by non-physical excitement of the induction coil and that do not subside to its zero value before reappearing will not be allowed to proceed through the rest of the analyzing circuit and thus will not cause an alarm to be produced.

To overcome the problem of repeated sirens during periods of extended sensor input, such as in the train passing example, or even when a truck or other heavy vehicle passes a parked car, means are provided to prevent repeated alarms as long as the initial input remains within a given intensity for an extended time. For instance, as long as the intensity level of the input signal remains rather constant following cessation of the full alarm signal, the circuit will not process another sensor input. This means that the prolonged motion of the train or sensor input from a slow moving truck passing a car will not cause the alarm to sound again. This feature also prevents continuous alarm outputs in those cases when the input causes the input sensor to go into unabated oscillation. This input may be mechanical in nature (the train example) or from electrical disturbances.

In a second embodiment of this invention, the circuit is designed such that fewer wires need be used to attach the sensor to the alarm giving rise to a savings in material and reduction in installation time and training.

The prior art has recognized some of these problems, however, to date there has been little success achieved in solving them. In the patent to Hwang, (U.S. Pat. No. 5,084,967) a "motion detector" is allegedly connected to a pair of signal amplifier circuits that, upon receipt of a long signal or a series of short pulses from the detector, will sound a "full" alarm whereas, upon receipt of a shorter pulse signals, will sound a "pre-entry warning", lesser in severity than the "full" alarm. However, close examination of this patent discloses that the "detector" is merely a switch that is purely time-dependent so that the signal must be either of long duration or short duration to actuate the circuit. While in the block diagram shown in the patent there is a call for a "signal amplifier circuit", the schematic shows merely the use of components that are arranged as a switch to turn on and off a transistor to let the detected signal pass on to the alarm warning device. Thus, there is no comparison of the "level of intensity" of the signal but merely the "duration" of the signal notwithstanding its intensity. This is not an accurate assessment of a threat signal and does not detect between "intensities" nor between physical and non-physical inputs and therefore is lacking. In addition, the output signal from this prior art device goes directly to the signaling device (siren) whereas the instant invention interposes another device, the alarm control module, that determines what type of alarm is to be generated.

Accordingly, the main object of this invention is a method and apparatus for use on an electronically secured vehicle that responds differently to different intensities of shock received by the vehicle. Other objects of the invention include a method and apparatus that has at least two levels of intensity determination, one for a relatively light shock received by the vehicle to produce a pulse that may be used to trigger a warning of a stronger alarm should the shock not be discontinued and a separate pulse that may be used to trigger a stronger, louder alarm for non-discontinued light

5,532,670

5

shocks and stronger shocks; a method and apparatus for producing a pulse that may be used to trigger a warn-away audible alarm that may be repeatedly sounded to signify the vehicle is under electronic security while not producing a pulse that may trigger the loudest alarm so as to minimize the disturbance to those nearby in the event of a non-threatening shock received by the vehicle; a method and apparatus that maintains readiness to produce a pulse that may be used to trigger an audible alarm even while a warn-away alarm message is being used; a method and apparatus for detecting a signal produced by a non-physical assault on the vehicle, such as by a burst of RF energy or EMF energy, and for removing it from further interaction in the system circuitry; a method and apparatus that provides full wave rectification of the induced signal in the induction coil to provide a more accurate analysis of the induced signal regardless whether the magnet initially moves away from the coil or toward it; an apparatus that may be retrofitted into existing vehicles as well as included as original equipment on new vehicles; and, an apparatus that will automatically rearm upon the completion of a measured length of the warn-away or the security-threatening alarm. These and other objects of the invention may be obtained by reading the following specification along with the drawings that are appended hereto. The protection sought by the inventor may be gleaned from a fair reading of the claims that conclude this specification.

DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic diagram of the apparatus using the method that provides the features of this invention;

FIG. 2 is a flow diagram illustrating the operation of the apparatus generally depicted in FIG. 1;

FIG. 3 is a schematic diagram of an alternate embodiment of the apparatus showing less wiring needed to accomplish the same functions as shown in FIG. 1;

FIG. 4 is a flow diagram of a portion of that shown in FIG. 2;

FIG. 5 is a schematic diagram of an alternate embodiment of the bilateral switch wiring shown in FIG. 1; and,

FIG. 6 is a schematic diagram of an alternate embodiment of the bilateral switch wiring shown in FIG. 3.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The novel method of this invention for indicating the threat level of an incoming shock to an electronically secured structure, such as a vehicle comprises, the steps of sensing a shock delivered to the vehicle, generating an electric signal the strength of which is proportional to the intensity of the shock, ignoring the first portion of the signal so as to remove from further consideration those shocks that are non-physical, analyzing the remaining signal to determine if it is of a low, generally non-threatening intensity or a higher, generally security-threatening intensity, and producing either a first pulse that triggers a low intensity "warn away" alarm, or separate first and second pulses, representing a signal containing both the low intensity and higher intensity components, that trigger both a low and a high intensity alarms. The step of generating an electric signal includes generating an alternating current signal whose amplitude and length is proportional to the intensity of the physical shock. FIG. 1 shows the apparatus of this invention.

6

In FIG. 1 the solid lines between components refer to conductors and will not be individually numbered except where necessary. Where conductors cross and the intersection is marked with a dot or period, it is a junction; where one conductor crosses another and the intersection has no dot or period, there is no junction. As shown in FIG. 1, an input voltage, generally in the range of from about six to about eighteen volts (d.c.), is inputted from a battery (not shown), such as a car battery or other source of direct current, to an input terminal 1. The current is regulated by a reverse flow protection diode 3, a surge limiting resistor 5, an over-voltage protection Zener diode 7 and a filter capacitor 9 to produce a steady flow of direct current. The ground return enters at input terminal 11.

The step of sensing a mechanical shock delivered to the vehicle is performed by a sensor 12 comprising a permanent magnet 13, about which a continuous magnetic field exists, and is suspended in a conventional elastic mount (not shown), such as between a pair of rubber bands anchored to a pair of spaced-apart posts (not shown) that rest on a solid base, such as the security sensor housing (not shown). Magnet 13 will detect an incoming shock and begin to vibrate back and forth in the mount in proportion to the intensity of the shock. That is to say, for light or low intensity shocks, magnet 13 will vibrate only a small amount and the vibrations will soon attenuate, while for higher intensity shocks, the vibration will be greater and last longer.

Nearby is fixedly positioned an induction pickup coil 15. The step of generating an electric signal, the strength of which is proportional to the intensity of the shock, is performed by the variation of the magnetic field from the vibrations magnet 13 inducing an alternating current in a coil 15 that produces an alternating voltage or signal.

The step of analyzing the signal to determine if it is of a low or high intensity includes the first step of passing the signal through a switching capacitor amplifier 19 to provide full wave rectification, i.e., the negative portions of the signal are converted to positive portions. According, the output of amplifier 19 is always positive and will give an approximately equal output no matter the direction of the impact to the vehicle so as to iron out the difficulties herein before exhibited when the impact to the vehicle causes magnet 13 to initially move away from coil 15. The gain of amplifier 19 is fixed at a predetermined value. Potentiometer 23 is used to adjust the level of the input from sensor 12.

An analog bilateral switch 101 is provided. It is opened a few, i.e. 5 milliseconds of each pulse string, as will be hereinafter more fully set forth, in order to cut off the first portion of the signal output from amplifier 19. This cut off is to prevent extraneous, nonphysical energy surges, such as from EMF fields, as hereinbefore described, from tripping the alarm.

Shutting off switch 101 is accomplished by use of an inverting comparator 111 and its associated circuitry. Resistors 105 and 107 establish a reference voltage for comparator 111. Resistor 103 and capacitor 109 filter out high frequency transients on the input to comparator 111. As a signal inputted to comparator 111 goes high, the output goes low and is coupled through a diode 113 and a capacitor 115 to switch 101. By adjusting the capacitance of capacitor 115, a delay, such as 5 milliseconds is required to charge capacitor 115 in order to turn on bilateral switch 101. Resistor 117 is provided as the discharge resistor for capacitor 115 and its value is chosen so that capacitor 115 will not discharge for several hundred milliseconds so as not to interrupt the signal pulse string. The discharge time of capacitor 115 is such that

5,532,670

7

only the first few milliseconds of any pulse string is allowed to be coupled through capacitor 115 and diode 113 to shut off analog bilateral switch 101.

The next step, after passing the amplified signal through switch 101 is to input this amplified signal simultaneously to two separate and independent voltage integrators, 29 and 31, shown within dotted line perimeters, that are paralleled from the output of amplifier 19. Integrator 29 comprises a resistor 33 and a capacitor 35 while integrator 31 comprises a resistor 37 and a capacitor 39. The ratio of sensitivity of integrators 29 and 31 is adjusted, by varying the resistance of resistors 33 and 37 and varying the capacitance of capacitors 35 and 39 to the order of approximately 5:1 so that integrator 29 is approximately five times as sensitive as integrator 31. This ratio can be varied outside of 5:1 under certain circumstances such as where the vehicle is unusually large.

The next step is to send the output of integrators 29 and 31 to a pair of separate voltage comparators/pulse generators 41 and 43 that are equally referenced from input terminal 1. The reference for voltage comparator 41 is established by resistors 45 and 47 and a diode 49 while the reference for voltage comparator 43 is established by resistors 51 and 53 and a diode 55. Another pair of diodes 57 and 59 are used to latch the respective voltage comparators 41 and 43 when their respective input signals exceed the comparator reference voltages.

The next step in this novel method is for the pulse generator portion of comparators/generators 41 and 43 to output either a first pulse from generator 41 representing a low intensity signal or separate first and second pulses from both generators 41 and 43 representing a signal containing a low intensity and a high intensity component. This is performed when voltage comparator 41 or 43 is latched through either diode 57 or diode 59 when the incoming signal from integrators 29 or 31 exceeds the reference voltage thereto. Once latched, the respective comparator produces an output pulse timed by resistor 45 and capacitor 61 with respect to comparator/pulse generator 41 or by resistor 51 and a capacitor 63 with respect to comparator/pulse generator 43 to one of two drive transistors 65 and 71.

Output drive transistor 65 receives the output pulse from voltage comparator/pulse generator 41 through a resistor 67 and an indicating light emitting diode 69 for the duration of the pulse from generator 41. The other output drive transistor 71 receives the output pulse from voltage comparator/pulse generator 43 through a resistor 73 and an indicating light emitting diode 75 for the duration of the pulse from generator 43. Resistors 77 and 79 are current limiting resistors to protect transistors 65 and 71 respectively. The outputs are enabled by a ground placed on terminal 81 through a diode 83. The outputs are fed respectively to terminal 85 to connect to a warn-away alarm circuit (not shown), and to terminal 87, to connect to the full alert alarm circuit (not shown). The output pulse for the warn-away alarm, from terminal 85, may be set at one length, such as 200 milliseconds, and the output pulse for the full alarm from terminal 87 may be set at a different length, such as approximately 1 full second.

The negative 5 millisecond pulse from comparator 111 is inverted by inverter 123. This pulse resets and holds in reset for the 5 millisecond period the "D flip-flop" 125. The "Q" output of 125 is connected to the inputs of "AND-GATES" gates 151 and 165, causes the outputs of 151 and 165 to go low. The low signals at the outputs of 151 and 165 opens normally closed analog bilateral switches 127 and 129. This

8

prevents any output from pulse generators 41 and 43 from being coupled to output transistors 65 and 71.

After the end of the 5 millisecond reset pulse, the "Q" output at flip-flop 125 is set high by a clock signal created by comparator 111. This clock pulse is inverted by inverter 121 to present the proper input to the 125 clock input. The sensor outputs 85 and 87 are now enabled for the duration of the output pulse(s) created by pulse generators 41 and 43.

Output bypass timers 143 and 157 are triggered and reset from the trailing edge (negative going edge) of the output pulses from pulse generators 41 and 43 respectively. The output of full alarm pulse generator 43 is applied to timer 157 via AND-GATE 173. When any input of an AND gate goes low, its output goes low. All inputs of an AND-GATE must be high to get a high at its output. These triggers are coupled to the inputs of the timers by coupling capacitors 141 and 155 respectively. Resistors 139 and 153 are pull-up resistors on the trigger input of their respective timers. Resistor 145 and capacitor 149 control the time that the "warn-away" output is disabled. Resistor 159 and capacitor 163 control the time that the "alarm" output is disabled. When the timers are triggered/reset, the timing capacitors 149 and 163 are discharged, the outputs go high, and the timing cycle is started. The outputs will go low at the end of the timing cycle.

The high output from warnaway bypass timer 143 is inverted by inverter 147 and applied to AND-GATE 151. The low at the input of 151 causes the output of 151 to go low opening bilateral switch 127. This interrupts any output from pulse generator 41 and disables the warnaway output drive to output transistor 65. All warnaway outputs are therefore disabled anytime that warnaway bypass timer 143 is running. All repetitive triggers that occur inside the timing window are bypassed (disabled) on the warnaway output until the warnaway bypass timer expires (approximately 1/2 second). While the timer is running, if the output at pulse generator 41 goes low (output pulse expires), the timing capacitor is discharged, and the timer is restarted with a full charging cycle duration to run.

Full alarm bypass timer 157, upon receiving a negative pulse from the trailing edge of the output pulse from pulse generator 43 via AND-GATE 173, works identical to the warnaway bypass timer 143. The high output from 157 is inverted by inverter 161 and applied to AND-GATES 151 and 165. The low at the inputs of 151 and 165 causes the outputs of 151 and 165 to go low. This low output in turn is applied to the control input of bilateral switches 127 and 129. Both output drives are interrupted, disabling both outputs (warnaway and full alarm) for the duration of the full alarm output bypass timer 157 (several seconds).

The full alarm bypass timer 157 is also used as a power up reset timer. At power on capacitor 171 is fully discharged, applying a low at the input of AND-GATE 173. Capacitor 171 is slowly charged through bias resistor 169 removing the low input from AND-GATE 173. The output of 173 is low during this charging period triggering full alarm bypass timer 157. Therefore, at power up, both outputs are disabled for several seconds until timer 157 times out.

FIG. 2 shows the flow of the induced signal and produced pulse through the circuit of FIG. 1. FIG. 4 is a flow diagram of a portion of FIG. 2. The magnet 13 and coil 15 components pick up the incoming shock and generate a signal the strength of which is proportional to the intensity of the shock. Amplifier 19 provides full wave rectification and amplification of the signal for presentment through switch 101 to integrators 29 and 31 in parallel for integration of the

5,532,670

9

total value of the pulse train less the first part thereof cut off by switch 101. The respective sensitivities of integrators 29 and 31 help to differentiate between a light shock that in all probability is non-threatening in nature and a heavier shock that represents a potential intrusion into the vehicle. The separate voltage comparators/output pulse generators 41 and 43 complete the differentiation and output a pulse to the output indicator and driver that results in one or both alarms being activated.

Amplifier 19, referenced by voltage from the car battery, will amplify all shocks received by the vehicle. Integrators 29 and 31 will ignore any signal whose peak-to-peak voltage is equal to or less than the amplifier reference voltage. Hence, very light shocks, although felt by magnet 13 and coil 15, will not produce a signal or signals sufficient to be activated by voltage comparators/output pulse generators 41 and 43 to latch the respective unit and produce a pulse to be sent on to output drive transistors 65 and 71.

Upon receipt of a light shock, above the reference level of amplifier 19, the circuit will operate to activate voltage comparator 41, latch it, and produce a pulse that will activate the warn-away alarm trigger output (not shown) through terminal 85. While this is going on, the circuit remains fully prepared to receive and process other shocks. Should a heavy shock be received while the warn-away alarm is given, the security breached alarm trigger output, will be tripped through terminal 87 and both alarms output will be tripped to go off simultaneously. In all cases, both alarm trigger outputs are tripped go off when a severe shock is received while only the warn-away alarm trigger output is tripped when a lighter shock is received.

FIG. 3 shows an alternate embodiment of the invention. By changing the timing of the full alarm pulse generator, to say 5 times the normal 200 milliseconds, allows for a considerable reduction in the output circuitry. This would also reduce the installation time of the sensor. With a 200 millisecond warnaway output pulse and one second full alarm pulse, these pulses can be outputted on the same wire for applying to one such input of the alarm control module.

To achieve a longer duty cycle for a full intensity alarm, full; alarm output pulse generator 43/timing capacitor 63 is changed to 5 times it's normal value. The full alarm output pulse time is therefore increased by a factor of 5.

The outputs from output pulse generators 41 and 43 are then applied to the common output indicating LED 69 and output drive transistor 65. This is accomplished via output drive current limiting resistors 67 and 73 and analog bilateral switches 127 and 129 connecting to a common conductor before reaching LED 69. Therefore the LED will indicate warnaway output with a short 200 millisecond light output pulse and full alarm output with a longer one second light output pulse. The output transistor 65 will be conducting applying a ground or near ground potential to the collector for 200 milliseconds for warnaway and for one second for full alarm.

This invention also carries the capability to drive the vehicle's electronic security system's audible or visual warning devices directly or indirectly by use of an external control relay. Since the warn-away output pulses are short (approximately $\frac{1}{4}$ of a second) and could be enabled by the vehicle's electronic security system, this would greatly reduce the annoyance created by an alarm system's full alarm. The output drivers have the capability to drive output control circuits as long as a ground is applied to output control terminal 81. These output pulses would be fed through output terminals 85 and 87 to directly or indirectly drive warning devices.

10

Although this invention is written in respect to a shock sensor, it is not limited to the same. The input to the protected vehicle could be sensed by any of the following detectors: shock, motion, shock/motion, audio discriminator, field disturbance, or other detector(s) with the proper input circuitry.

FIG. 5 represents a modification to the preferred embodiment shown in FIG. 1 and shows the output of the 5 millisecond timer 131 to invert the signal, by inverter 123, and feeding the output signal to two normally open, bilateral switches 100 and 102. The signal closes switches 100 and 102 for the 5 millisecond period. This also keeps integrator capacitors 35 and 39 shorted out for the 5 millisecond time period. This represents another method of handling the signal.

FIG. 6 represents a modification to the other preferred embodiment shown in FIG. 3 and also shows the output of the 5 millisecond timer 131 to invert the signal, by inverter 123, and feeding the output signal to two normally open, bilateral switches 100 and 102. The signal closes switches 100 and 102 for the 5 millisecond period. This also keeps integrator capacitors 35 and 39 shorted out for the 5 millisecond time period. This represents another method of handling the signal.

Also this unit is described as a 2-stage sensor, but the invention is not limited to 2 stages and may be employed with three (3) or more stages. The output pulses may vary in lengths such as 200 milliseconds for the "warnaway" and approximately one full second for the full alarm output. This will allow alarms with the capability to distinguish between "warnaway" and full alarm using one input. This will eliminate one drive transistor and one wire.

While the invention has been described by reference to a particular embodiment thereof, those skilled in the art will be able to make various modifications to the described embodiment of the invention without departing from the true spirit and scope thereof. It is intended that all combinations of elements and steps which perform substantially the same function in substantially the same way to achieve the same results are within the scope of this invention.

What is claimed is:

1. A method of indicating a threat level of an incoming shock to an electronically secured vehicle comprising the steps of:
 - a) sensing a shock delivered to the vehicle;
 - b) generating a signal having strength proportional to the intensity of said shock;
 - c) analyzing said signal to determine if it has a low, generally non-threatening intensity or a higher, generally security-threatening intensity; and
 - d) producing either a first pulse, representing that said signal has only said low intensity, or separately producing said first pulse and a second pulse, representing that said signal has both said low intensity and said higher intensity.
2. The method of claim 1 wherein the step of generating said signal includes the step of generating an alternating current signal having an amplitude proportional to said intensity of said shock.
3. The method of claim 1 wherein the step of analyzing said signal includes the steps of:
 - a) amplifying said signal to produce an amplified signal;
 - b) impressing said amplified signal simultaneously to at least two separate integrators of different sensitivity to produce integrated signals; and

5,532,670

11

c) activating a pulse generator specific to each of said integrated signals, if the associated integrated signal reaches a predetermined level.

4. The method of claim 1 wherein the step of analyzing said shock signal includes the steps of:

a) amplifying said signal to produce an amplified signal;

b) impressing said amplified signal simultaneously to at least two separate integrators of different sensitivity to produce integrated signals;

c) impressing said integrated signals simultaneously to at least two separate comparators of different sensitivity to produce a first comparator signal, if said integrated signals reach a first predetermined level, indicating said non-threatening intensity signal or a second comparator signal, if said integrated signals reach a second, higher predetermined level, indicating said higher threatening intensity signal; and

d) activating a pulse generator specific to said first and said second comparator signals.

5. The method of claim 1 wherein the step of analyzing said shock signal includes the steps of:

a) amplifying said signal to produce an amplified signal;

b) impressing said amplified signal simultaneously to at least two separate integrators/comparators, each said integrator/comparator having different sensitivity; and

c) activating a pulse generator to produce said first and said second pulses specific to each signal integrated and compared if that signal reaches an associated predetermined level.

6. The method of claim 1 wherein said step of analyzing said signal includes the steps of:

a) amplifying said signal to produce an amplified signal;

b) impressing said amplified signal simultaneously to at least two separate integrators of different sensitivity, to produce integrated amplified signals;

c) impressing said separate integrated, amplified signals to at least two signal comparators, one in series with each said integrator having different sensitivity to provide a first comparator signal indicating said non-threatening intensity signal or a second comparator signal indicating said higher threatening intensity signal; and

d) activating a pulse generator specific to each said comparator signal if said integrated, amplified signal reaches an associated predetermined level.

7. The method of claim 1 including the additional step of ignoring the first few milliseconds of said signal produced by a shock sensing device to eliminate spurious, nonphysical signals produced by random EMF energy fields interacting with said shock sensing device.

8. The method of claim 1 wherein the step of providing either said first pulse or said second pulse includes sending said pulses over a single conductor to an alarm control.

9. The method of claim 1 including the additional step of ignoring any signal produced by nonphysical energy.

10. The method of claim 9 wherein said nonphysical energy includes an EMF field.

11. The method of claim 1 wherein the step of analyzing said signal includes the additional steps of amplifying and rectifying the full wave of said signal so that said output represents all values of said signal, is solely positive, and reduces the differential in the positive and negative aspects of said signal that are produced when a magnet swings away from an inductor coil before swinging toward said coil.

12. The method of claim 1 wherein said second pulse has a pulse-width greater than a pulse-width of said first pulse.

12

13. An electronic vehicle security system for indicating a threat level of an incoming shock to an electronically secured vehicle comprising:

a) means for sensing a shock delivered to the vehicle;

b) means for generating a signal having strength proportional to the intensity of said shock;

c) means for analyzing said signal to determine if it has a low, generally non-threatening intensity or a higher, generally security-threatening intensity; and

d) means for providing either a first pulse representing that said signal has only said low intensity or separately providing said first and a second pulse, representing that said signal has both said low intensity and said higher intensity signal.

14. The electronic vehicle security system of claim 13 further including means for ignoring the first few milliseconds of said signal produced by said shock sensor to eliminate spurious, nonphysical signals produced by random EMF energy fields interacting with a shock sensing device.

15. The electronic vehicle security system of claim 13 further including means for sending said first and second pulses over a single conductor to an alarm control.

16. The system of claim 13 wherein said means for sensing a shock delivered to said vehicle includes a permanent magnet, having a magnetic field thereabout, suspended in an elastic mount on said vehicle for vibrating in said mount in response to said shock.

17. The system of claim 16 further including an induction coil fixedly mounted near said magnet for receiving a vibrating magnetic field therein to produce an induced alternating current and voltage therein.

18. The system of claim 17 further including a capacitor through which said induced alternating current and said voltage are passed to remove direct current and voltage therefrom.

19. The system of claim 17 wherein said means for analyzing said signal includes:

a) a signal amplifier, having an output therein, for receiving said induced alternating current and voltage from said induction coil and providing an amplified signal thereof; and

b) first and second voltage integrators connected to said amplifier output, said first integrator having a high sensitivity for responding to said non-threatening intensity signal and said second integrator having a lower sensitivity for responding to said higher intensity signal, said integrators simultaneously receiving said amplified signal from said amplifier.

20. The system of claim 19 wherein said means for providing either said first pulse or said separate first and second pulses include a pair of voltage comparators/output-pulse-generators, one connected to each said voltage integrator for comparing integrated voltages produced from each said integrator and providing said first pulse representing said low intensity signal from said high sensitivity integrator and providing both said first and said separate second pulse representing said low intensity signal from said high sensitivity integrator and said high intensity signal from said low sensitivity integrator.

21. The system of claim 17 wherein said means for analyzing said signal includes:

a) a signal amplifier, having an output therein, for receiving said induced alternating current and voltage from said induction coil and providing an amplified signal thereof; and

b) first and second voltage comparators connected to said amplifier output, said first comparator having a high

5,532,670

13

sensitivity for responding to said non-threatening intensity signal and said second comparator having a lower sensitivity for responding to said higher intensity signal, said integrators simultaneously receiving said amplified signal.

22. The system of claim 17 wherein said means for analyzing said signal includes:

- a) a signal amplifier, having an output therein, for receiving said induced alternating current and voltage from said induction coil and providing an amplified signal thereof; and
- b) first and second voltage integrators and comparators connected to said amplifier output, said first integrator and comparator having a high sensitivity for responding to said non-threatening intensity signal and said second integrator and comparator having a lower sensitivity for responding to said higher intensity signal, said integrators and comparators simultaneously receiving said amplified signal from said amplifier.

23. The electronic vehicle security system of claim 13 further including means for ignoring any signal produced by nonphysical energy.

24. The electronic vehicle security system for indicating the threat level of an incoming shock to an electronically secured vehicle of claim 23 wherein said nonphysical energy includes an E F field.

25. The electronic vehicle security system of claim 13 wherein said second pulse has a pulse-width greater than a pulse-width of said first pulse.

26. A method of blocking spurious signals produced by a shock sensor in a motor vehicle anti-theft system from interaction between extraneous bursts of RF energy and a sensor induction coil, comprising the steps of:

- a) amplifying a signal produced by a shock sensor to produce an amplified signal;
- b) inputting said amplified signal to a comparator and comparing an output signal of said inverter/comparator against a known reference; and
- c) outputting said amplified signal to an analog bilateral switch through a capacitor so that the charging of said capacitor will open said switch a few milliseconds to delete the front end of said amplified signal and remove it from further consideration.

27. The method of claim 26 wherein the step of amplifying said signal includes the additional steps of amplifying and rectifying a full wave of said signal so that said amplified signal represents all values of said signal, is solely positive, and reduces the differential of the positive and negative aspects of said signal that are produced when a magnet swings away from an inductor coil before swinging toward said coil.

28. A method of indicating the threat level of an incoming shock to an electronically secured vehicle including a magnet and an induction coil arranged as part of a shock sensor comprising the steps of:

- a) sensing a shock delivered to the vehicle including the step of generating an alternating current signal having amplitude proportional to the intensity of said shock;
- b) analyzing said signal to determine if it is of a low, generally non-threatening intensity or a higher, generally security-threatening intensity, including the steps of:
 - i) rectifying and amplifying said signal;
 - ii) impressing said rectified, amplified signal simultaneously to at least two separate integrators of different sensitivity;

14

iii) impressing said separate integrated, amplified signals to at least two signal comparators of different sensitivity, one in series with each said integrator; and

iv) activating a pulse generator responsive to an output of each signal comparator; and

c) providing either a first pulse representing a low intensity signal, or separate first and second pulses representing said signal containing both low intensity and higher intensity components.

29. The method of claim 28 including the additional step of ignoring the first few milliseconds of said signal to eliminate spurious signals produced by random EMF energy fields interacting with said shock sensor.

30. The method of claim 28 wherein the step of providing either said first pulse or said second pulse includes sending said pulses over a single conductor to an alarm control.

31. The method of claim 28 including the additional step of ignoring nonphysical signals interacting with the shock sensing device.

32. The method of claim 31 wherein said nonphysical signals include EMF energy fields.

33. The method of claim 28 wherein said second pulse has a pulse-width greater than a pulse-width of said first pulse.

34. An electronic vehicle sensor for indicating the threat level of an incoming shock to an electronically secured vehicle comprising:

- a) means for sensing a shock delivered to a vehicle including a permanent magnet, having a magnetic field thereabout, suspended in an elastic mount on said vehicle for vibrating in said mount in response to said shock;
- b) means for generating a signal the strength of which is proportional to the intensity of said shock including an induction coil fixedly mounted near said magnet for receiving a vibrating magnetic field therein to produce an induced alternating current and voltage therein;
- c) a capacitor through which said induced alternating current and voltage are passed to remove direct current and voltage therefrom;
- d) means for analyzing said signal to determine if it is a low, generally non-threatening intensity or a higher, generally security-threatening intensity including:
 - i) a signal amplifier for receiving said induced alternating current and voltage from said induction coil; and
 - ii) a pair of voltage integrators connected to an output of said amplifier which produces an amplified signal, one said integrator having a high sensitivity for responding to said amplified signal containing only low intensity components and the other said integrator having a lower sensitivity for responding to said amplified signal containing higher intensity components, said integrators simultaneously receiving said amplified signal from said amplifier; and
- e) means for producing either separate first and second pulses representing said signal containing both said low intensity and said higher intensity component, or said first pulse representing said low intensity signal, including a pair of voltage comparators/output pulse generators, one connected to each said voltage integrator for comparing outputs produced from each said integrator and producing said first pulse representing said low intensity signal from said high sensitivity integrator and providing both said first and said separate second pulse from both said generators represent-

ing said low intensity signal from said high sensitivity integrator and a high intensity signal from said low sensitivity integrator.

35. The method of claim 34 wherein said second pulse has a pulse-width greater than a pulse-width of said first pulse. 5

36. A method of blocking spurious signals produced in a motor vehicle anti-theft system from interaction between extraneous bursts of EMF or RF energy and a sensor induction coil, comprising the steps of:

- a) amplifying signals produced by a shock sensor including amplifying a full wave of said signal providing an amplified signal and rectifying said amplified signal so that said amplified signal represents all values of said signal, is solely positive, and reduces the differential in the positive and negative aspects of said signal that are produced when a magnet swings away from an inductor coil before swinging toward said coil; 10
- b) outputting said amplified signal to an analog bilateral switch through a capacitor so that charging said capacitor will open said switch for a predetermined period of time to delete a front end of said amplified signal as it passes therethrough and remove said front end from further consideration; and 20
- c) inputting said amplified signal to a comparator and comparing it against a known value.

37. The method of claim 36 wherein said predetermined period of time is about 5 milliseconds.

38. A method of blocking spurious signals produced by a shock sensor in a motor vehicle anti-theft system from interaction between extraneous bursts of RF energy and a sensor induction coil, comprising the steps of:

- a) amplifying signals produced by a shock sensor to produce an amplified signal;
 - b) inputting said amplified signal to a comparator and comparing it against a known reference;
 - (c) ignoring said signal produced by said shock sensor for a predetermined period of time to eliminate spurious, nonphysical signals produced by random energy interacting with a shock sensing device and removing it from further consideration
39. The method of claim 38 wherein the step of ignoring said signal includes outputting said signal to an analog bilateral switch through a capacitor so that the charging of said capacitor will open said switch a few milliseconds to delete the front end of said signal and remove it from further consideration.

40. The method of blocking spurious signals produced by a shock sensor in a motor vehicle anti-theft system of claim 38 wherein said nonphysical signal includes an EMF field.

* * * * *

**Limited Lifetime
Consumer Warranty**

Directed Electronics, Inc. ("Directed") promises to the original purchaser to repair or replace with a comparable reconditioned model any Directed unit (hereafter the "unit"), excluding without limitation the siren, the remote transmitters, the associated sensors and accessories, which proves to be defective in workmanship or material under reasonable use during the lifetime of the vehicle provided the following conditions are met: the unit was professionally installed and serviced by an authorized Directed dealer; the unit will be professionally reinstalled in the vehicle in which it was originally installed by an authorized Directed dealer; and the unit is returned to Directed, shipping prepaid with a legible copy of the bill of sale or other dated proof of purchase bearing the following information: consumer's name, telephone number and address; the authorized dealer's name, telephone number and address; complete product description, including accessories; the year, make and model of the vehicle; vehicle license number and vehicle identification number. All components other than the unit, including without limitation the siren, the remote transmitters and the associated sensors and accessories, carry a one-year warranty from the date of purchase of the same. This warranty is non-transferable and is automatically void if: the original purchaser has not completed the warranty card and mailed it within ten (10) days of the date of purchase to the address listed on the card; the unit's date code or serial number is defaced, missing or altered; the unit has been modified or used in a manner contrary to its intended purpose; the unit has been damaged by accident, unreasonable use, neglect, improper service, installation or other causes not arising out of defects in materials or construction. The warranty does not cover damage to the unit caused by installation or removal of the unit. Directed, in its sole discretion, will determine what constitutes excessive damage and may refuse the return of any unit with excessive damage. **TO THE MAXIMUM EXTENT ALLOWED BY LAW, ALL WARRANTIES, INCLUDING BUT NOT LIMITED TO EXPRESS WARRANTY, IMPLIED WARRANTY, WARRANTY OF MERCHANTABILITY, FITNESS FOR PARTICULAR PURPOSE AND WARRANTY OF NON-INFRINGEMENT OF INTELLECTUAL PROPERTY, ARE EXPRESSLY EXCLUDED; AND DIRECTED NEITHER ASSUMES NOR AUTHORIZES ANY PERSON OR ENTITY TO ASSUME FOR IT ANY DUTY, OBLIGATION OR LIABILITY IN CONNECTION WITH ITS PRODUCTS. DIRECTED DISCLAIMS AND HAS ABSOLUTELY NO LIABILITY FOR ANY AND ALL ACTS OF THIRD PARTIES INCLUDING ITS AUTHORIZED DEALERS OR INSTALLERS. DIRECTED SECURITY SYSTEMS, INCLUDING THIS UNIT, ARE DETERRENENTS AGAINST POSSIBLE THEFT. DIRECTED IS NOT OFFERING A GUARANTEE OR INSURANCE AGAINST VANDALISM, DAMAGE OR THEFT OF THE AUTOMOBILE, ITS PARTS OR CONTENTS; AND HEREBY EXPRESSLY DISCLAIMS ANY LIABILITY WHATSOEVER, INCLUDING WITHOUT LIMITATION, LIA-**

© 2001 Directed Electronics, Inc.

BILITY FOR THEFT, DAMAGE AND/OR VANDALISM. THIS WARRANTY DOES NOT COVER LABOR COSTS FOR MAINTENANCE, REMOVAL OR REINSTALLATION OF THE UNIT OR ANY CONSEQUENTIAL DAMAGES OF ANY KIND. IN THE EVENT OF A CLAIM OR A DISPUTE INVOLVING DIRECTED OR ITS SUBSIDIARY, THE PROPER VENUE SHALL BE SAN DIEGO COUNTY IN THE STATE OF CALIFORNIA. CALIFORNIA STATE LAWS AND APPLICABLE FEDERAL LAWS SHALL APPLY AND GOVERN THE DISPUTE. THE MAXIMUM RECOVERY UNDER ANY CLAIM AGAINST DIRECTED SHALL BE STRICTLY LIMITED TO THE AUTHORIZED DIRECTED DEALER'S PURCHASE PRICE OF THE UNIT. DIRECTED SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO, ANY CONSEQUENTIAL DAMAGES, INCIDENTAL DAMAGES, DAMAGES FOR THE LOSS OF TIME, LOSS OF EARNINGS, COMMERCIAL LOSS, LOSS OF ECONOMIC OPPORTUNITY AND THE LIKE. NOTWITHSTANDING THE ABOVE, THE MANUFACTURER DOES OFFER A LIMITED WARRANTY TO REPLACE OR REPAIR THE CONTROL MODULE AS DESCRIBED ABOVE. Some states do not allow limitations on how long an implied warranty will last or the exclusion or limitation of incidental or consequential damages. This warranty gives you specific legal rights and you may also have other rights that vary from State to State.

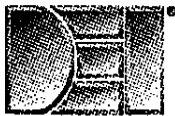
This product may be covered by a Guaranteed Protection Plan ("GPP"). See your authorized Directed dealer for details of the plan or call Directed Customer Service at 1-800-876-0800. Directed security systems, including this unit, are deterrents against possible theft. Directed is not offering a guarantee or insurance against vandalism, damage or theft of the automobile, its parts or contents; and hereby expressly disclaims any liability whatsoever, including without limitation, liability for theft, damage and/or vandalism. Directed does not and has not authorized any person or entity to create for it any other obligation, promise, duty or obligation in connection with this security system.

Make sure you have all of the following information from your dealer:

A clear copy of the sales receipt, showing the following:

- Date of purchase
- Your full name and address
- Authorized dealer's company name and address
- Type of alarm installed
- Year, make, model and color of the automobile
- Automobile license number
- Vehicle identification number
- All security options installed on automobile
- Installation receipts

Terms and Conditions for Authorized Dealers, Summary



Directed Electronics, Inc.

Purchase Agreement:

Amounts due as a result of any and all purchases hereafter made by Customer (Retailer) from Supplier (DEI) will be paid to Supplier on the following terms and conditions.

Terms

Before initial order can be shipped, the "Customer Information Form" and "Authorized Dealer Agreement" must be completed. C.O.D. Cash orders are not subject to credit limit, C.O.D. Company Check orders may be subject to credit limit if checks have been returned for redeposit. Open accounts with terms of net 30 days from date of invoice will be established only AFTER volume dealer level is established and credit application is reviewed and approved.

Late Payment

Subject to applicable laws, past due amounts are subject to late payment service charges of 1.5% per month, which is an annual rate of 18% or up to a maximum rate allowed by law. Accounts past due will have shipments held and may be placed on C.O.D. Legal action may be taken at any time.

Bad Checks

Any check returned for "Non Sufficient Funds" automatically changes the account terms to C.O.D. CASH (cashier's check, money order). A service charge of \$20.00 will be applied to each returned check.

Failure to Pay/Insolvency

Failure by Customer to pay any part of the purchase price when due, or in the event that proceedings in bankruptcy, receivership, or insolvency are instituted by or against Customer or his property, Supplier may, at its option, cause the entire unpaid balance to become due and immediately payable. Customer hereby expressly waives any right to any action which may accrue by reason of the entry for taking possession of or the selling of sold materials and to pay all costs incurred with respect thereto, including service charges, attorney's fees and court costs.

Entire Agreement

This Agreement covers all materials which Customer may hereafter acquire at any time from Supplier. No waivers or modifications shall be valid unless the same are in writing and executed by the parties hereto. This contract shall apply and accrue to the benefit of, and be binding upon, the heirs, executors, administrators, successors, and assigns of respective parties. Customer may not transfer or assign any rights or obligations under this agreement without the express written consent of Directed Electronics, Inc.

Litigation

In the event of any litigation arising out of this agreement, Supplier shall be entitled to its costs and expenses incurred including, without limitation, attorney's fees.

State Laws

This Purchase Agreement shall be governed by the laws of the State of California. Any dispute regarding this Agreement will be subject to the exclusive jurisdiction and venue of the courts of San Diego County, California.

Receipt of Copy

Customer hereby acknowledges the receipt of a copy of this Agreement at the time of its execution. _____
Initials

Order Errors and Returns

All errors must be reported within 10 days of the receipt of an order. Call DEI Returns to obtain a Returned Merchandise Authorization (RMA) Number BEFORE returning product for credit or mis-shipped product. RMA numbers are REQUIRED for all returned product EXCEPT for repair or replacement items under warranty. All items are returned at the Authorized Dealer's expense with invoice number identified.

RMA Number

The RMA number must be issued from DEI Headquarters. Complete information on Order/Invoice numbers, quantity/part numbers, reason for return, account name and number, contact person, and telephone number required to avoid delays.

Warranty Repairs

Refer to DEI's "Authorized Dealer Agreements and Conditions" (blue sheets) in this packet, page 8.

Restocking Fee

A restocking charge of 15% will be made on all goods returned unless due to Supplier's error.

Handling Fee

Orders less than \$350.00 (at invoice pricing) will be subject to a \$15.00 Handling Fee.

Title

Title to any and all goods or materials hereafter purchased shall remain with Supplier until the full purchase price has been paid.

Dealer Authorization:

1. Authorized Dealer's Functions

- 1.01 Appointment of Authorized Dealer: DEI agrees to appoint Authorized Dealer and Authorized Dealer agrees to serve as a non-exclusive retail Dealer, based upon the terms and conditions set forth in this agreement and only at the location set forth above or where applicable, the additional locations set forth in Schedule A to this agreement. In consideration of its appointment as a DEI Retail Dealer, the Authorized Dealer agrees to and shall:
 - A. Utilize its best efforts to promote and sell the authorized products within its specified market area.
 - B. Maintain quality facilities for on-premise demonstration and sale of DEI products.
 - C. Maintain an Installation Facility, owned, staffed and operated by the Authorized Dealer and which meets all requirements established by DEI.
 - D. Keep confidential any and all correspondence and/or material from DEI that is marked as such.
 - E. Sell Authorized Products installed only and only to end users.
- 1.02 The Authorized Product: The Authorized Dealer shall order and sell only the DEI product line(s) that have been authorized by this agreement. The authorized product line(s) authorized by this Agreement are _____

_____ These are the "Authorized Products."

2. Authorized Dealer Location

- 2.01 Authorized Dealer shall not offer to sell, transfer, hypothecate or otherwise dispose of any authorized DEI products to any person or entity other than the end consumer; and the Authorized Dealer shall not sell Authorized Products from any other location other than the approved location(s) listed in this agreement. Schedule "A" is used for additional Authorized Locations.
- 2.02 Authorized Dealer shall notify DEI of any change in location of business(es).

3. Advertising

Authorized Dealer shall not advertise or engage in promotion activities concerning any DEI products unless:

- A. Authorized Dealer has a sufficient supply of these products on hand to meet anticipated demand.
- B. All references to DEI's trademarks or tradenames shall state that the marks are the property of Directed Electronics, Inc.

4. Warranties

Authorized Dealer shall honor DEI's published warranty to all customers to whom the Authorized Dealer sells or has sold DEI products. Authorized Dealer shall make no warranties or guarantees with respect to products or to use of products except as authorized by DEI in writing. Sales shall be made under DEI's warranty in effect at the time of sale. Authorized Dealer shall furnish to each retail purchaser all warranty cards or similar material provided by DEI.

5. Nationwide Assistance Program

- 5.01 From time to time, a DEI customer may be traveling throughout the country. If this customer should happen to be a long distance (more than 75 miles) from the DEI Dealer that originally installed the product and experience a problem with a DEI product, he qualifies for our Nationwide Assistance Program. To maintain a Nationwide Assistance Program for all DEI customers, all DEI Authorized Dealers shall provide Warranty Assistance to any DEI Customer traveling in their local area, provided:
 - A. The DEI product was installed by an Authorized Dealer.
 - B. The customer is more than 75 miles away or outside the original sales market area from the installing Authorized Dealer.
 - C. The product in question is under DEI warranty.
 - D. The servicing Authorized Dealer is authorized to sell the product line in question.
- 5.02 Provided the customer meets the above listed requirements, the Authorized Dealer shall honor the DEI warranty on the product in question and provide the customer with:
 - A. Free diagnosis of system problem (limited to product failure only). In cases of installation problems, Authorized Dealer may charge the customer its normal labor rates.
 - B. Replacement (provided the Authorized Dealer has the component in question in stock) or bypass of defective component(s).
 - C. In case Authorized Dealer does not have the necessary parts, Authorized dealer shall use best efforts to obtain such parts.

Terms and Conditions for Authorized Dealers, Summary**Dealer Authorization (continued):**

- 5.03 If the customer cannot provide proof that they are eligible for the Nationwide Assistance Program or provided no failure or defect is found, the Authorized Dealer reserves the right to charge this customer any and all of its normal charges.
- 5.04 Notwithstanding any of the above, DEI shall have no obligation to pay the Authorized Dealer for any of its costs, fees or expenses.

6. Term and Termination

- 6.01 Either party may terminate this agreement at will and without cause, effective immediately upon written notice being delivered to the other party.
- 6.02 As of the effective date of termination, unfilled Authorized Dealer orders shall be deemed canceled and for thirty (30) days from that date DEI shall have the option to purchase from the Authorized Dealer and the Authorized Dealer agrees to sell to DEI all or any part of the DEI products then in the Authorized Dealer's stock at the prices the Authorized Dealer paid for the product less any discounts and unearned allowances paid to the Authorized Dealer. Upon exercise of this option, the Authorized Dealer shall ship the DEI products to DEI at DEI's expense.
- 6.03 As of the effective date of termination, the Authorized Dealer shall refrain from selling any previously Authorized Products and from any conduct which would make it appear that it is an authorized DEI Dealer. Authorized Dealer shall promptly remove from its letterheads, advertising literature, promotional materials, signage and from all telephone and other business directories of any kind all references to the DEI, its products or marks. Authorized Dealer shall promptly refrain from acting as an Authorized Dealer with respect to the products or on behalf of DEI and thereafter shall not use any corporate name, trade name or trademark tending to give the impression that any relationship still exists between DEI and the Dealer. The Dealer agrees to ship to DEI, all advertising, sales and promotional materials bearing DEI's products, names or marks.

7. Miscellaneous

- 7.01 **Non-Assignment:** Authorized Dealer shall not have the right to assign, transfer, hypothecate or sell its rights under this Agreement and any such assignment, transfer or sale of rights by Authorized Dealer shall be null and void ab initio unless approved in writing by DEI.
- 7.02 **Indemnification:** Authorized Dealer shall indemnify and hold DEI harmless from and against any and all claims, damages, judgments, decrees, orders and liabilities whatsoever, asserted by any person or entity resulting directly or indirectly from any act, omission or commission by the Authorized Dealer and such indemnification shall include the payment of all expenses, costs and attorney's fees expended by DEI in defending such claims.
- 7.03 **Governing Law:** This agreement is deemed to have been entered into in Vista, California, and shall be governed by the laws of the State of California. All questions concerning validity, interpretation, or performance of any of the terms of this Agreement, or determination of any rights or obligations of the parties thereto, shall be resolved or litigated in courts in San Diego County, California, regardless of where the Agreement is executed, and shall be governed by the laws of the State of California, without regard to conflicts of laws. In the event of any action or proceeding, including arbitration, to enforce this agreement or any of its provisions, or to declare the rights of the parties with respect to this Agreement, the prevailing party shall be entitled to its Attorney's fees, expenses and court costs.
- 7.04 **Severability:** If any provisions of this agreement are held unenforceable or invalid for any reason whatsoever, such unenforceability or invalidity shall not affect the enforceability of the remainder of this Agreement. Any such unenforceable or invalid provision shall be severable from the remainder of this Agreement, which shall remain enforceable.
- 7.05 **No Waivers or Modifications:** No waivers or modifications of this Agreement shall be enforceable unless the same are made in writing and executed by all parties.
- 7.06 This agreement shall be deemed jointly drafted and no ambiguities, duties or obligations shall be resolved against the drafting party.
- 7.07 The owners and/or proprietors of the Authorized Dealer shall be jointly and severally liable under the terms, rights and obligations of this agreement.

Personal Guaranty:

1. As employed herein "credit" means financial accommodation of any kind, and "indebtedness" includes all obligations of the Debtor to the Creditor, alone or with others, hereafter incurred, voluntarily or involuntarily, due or not due, absolute, inchoate, contingent, liquidated or unliquidated, and interest on each such obligation as provided in the note or other instrument representing the same, or, if none, then interest at the maximum statutory rate of interest.
2. Without further authorization from or notice to the Guarantor, Creditor may grant credit to the Debtor from time to time, either before or after revocation hereof and in such manner, on such terms, and for such term and for such time as it deems best; and with or without notice to the Guarantor, Creditor may alter, compromise, accelerate, extend or change the time or manner for the payment of any indebtedness; increase or reduce the rate of interest thereon; release or add any one or more guarantors or endorsers, accept additional or substituted security, or release or subordinate any security. No exercise or

non-exercise by Creditor or any right hereby given to it; no dealing by Creditor with Debtor or any guarantor or endorser; no change, impairment or suspension of right or remedy of Creditor shall in any way affect any of the Guarantor's obligations hereunder or any security furnish hereunder by the Guarantor or give the Guarantor any recourse against the Creditor.

3. The Guarantor, jointly and severally, unconditionally and continuously guarantee and promise to pay to Creditor or its order, each item of indebtedness hereby guaranteed and to perform each guaranteed obligation when due. The respective obligations of the Guarantor shall not be subject to proration.
4. In addition to all liens and rights of set-off which Creditor may have against any property of the Debtor or of the Guarantor, Creditor shall have a general lien on and a right to set-off against all the property of the Guarantor now or hereafter in the possession of or on deposit with the Creditor. Each such lien or right of set-off may be exercised with or without demand upon or notice to any of the Guarantor; and shall continue to full force unless specifically waived or released by Creditor, in writing, and shall not be deemed waived by any conduct of Creditor, or by any failure to exercise such right.
5. Creditor need not take any action against the Debtor, any other guarantor, or any other person, firm or corporation or resort to any security held by it at any time before proceeding against any of the Guarantor.
6. Until all indebtedness herein guaranteed has been paid in full, the Guarantor shall not assert any right of subrogation unless expressly authorized in writing by Creditor.
7. All existing and future indebtedness owing by the Debtor to any of the Guarantor is hereby subordinated to all debts and obligations hereby guaranteed; and without prior consent of Creditor, shall not be paid to the Guarantor by the Debtor in whole or in part during the life of this guaranty. Any payment by the Debtor to any of the Guarantor in violation of the foregoing provision shall be held by the Guarantor as trustee for the Creditor and paid over to the Creditor on its order.
8. The failure of the Creditor to file or enforce a claim against the estate of the Debtor, either in assignment, under the Bankruptcy Act or any other proceeding, shall not affect the liability of the Guarantor; nor shall the Guarantor be released from liability if recovery from the Debtor, any other guarantor, or any other person, becomes barred by any statute of limitations or is otherwise prevented. The Guarantor waives and agrees not to assert or take advantage of the defense of the Statute of Limitations in any action hereunder, or for the collection of any credit hereby guaranteed.
9. The Guarantor will file any claim against the Debtor in any bankruptcy or other proceeding in which filing of claims is required by law upon any indebtedness of the Debtor to the Guarantor and will assign to the Creditor all rights of the Guarantor thereunder. If the Guarantor does not file such claim or claims, Creditor is hereby authorized as our attorney in fact for such purpose hereby appointed, to do so in our name or in the Creditor's discretion, to assign the claim to and cause Proof of Claim to be filed in the name of the Creditor's nominee. In all such cases, the person or persons authorized to pay such claim shall pay to the Creditor the full amount payable on the claim in the proceeding before making any payment to the Guarantor; and to the full extent necessary for that purpose, the Guarantor hereby assigns to the Creditor their respective rights to any payments or distributions to which the Guarantor would otherwise be entitled.
10. With or without notice to the Guarantor, Creditor, in its sole discretion, may apply all payments from the Debtor, any of the Guarantor, any other guarantor, or realized from any security in such a manner and order of priority as the Creditor sees fit, to any obligation of the Debtor, whether or not such obligation is due at the time of such application.
11. In the event that action or other proceedings shall be brought to enforce this guaranty or any provision thereof, the same may be maintained alone, or joined with any action or other proceeding against the Debtor or any other guarantor of the Debtor's obligations to the Creditor. Prior action or suit against the Debtor, whether alone or jointly with other guarantors, shall not be prerequisite to Creditor's right to proceed hereunder or otherwise against the Guarantor or by any number of successive actions until and unless all indebtedness hereby guaranteed has been paid or performed and each of the Guarantor's obligations hereunder have been fully satisfied.
12. This is a continuing guaranty. Notice of its acceptance is waived and it shall remain in full force and effect until the Guarantor, respectively, in accordance with paragraph 19 of this Agreement, deliver(s) to Creditor written notice revoking it as to indebtedness incurred to such delivery.
13. The Guarantor agrees to pay to the Creditor all amounts necessary to enforce this guaranty against the Guarantor through Creditor's collection agent or Creditor's attorney.
14. Should any one or more of the provision of the guaranty be determined to be illegal or unenforceable, all other provisions nevertheless shall remain effective.
15. In the event a dispute arises between the Creditor and the Guarantor or the Creditor and the Debtor, the parties shall adjudicate their dispute in San Diego County, in the State of California pursuant to the laws of the State of California. The prevailing party shall be entitled to costs and attorney fees.
16. This agreement shall inure to the benefit of the Creditor, its successors and assigns; and shall bind the assigns and administrators of the Guarantor.

Terms and Conditions for Authorized Dealers, Summary

Personal Guaranty (continued):

17. The obligations of all guarantors hereunder shall be joint and several.
18. If the Guarantor comes into possession of any Products which Creditor hereafter ships to Debtor, the Guarantor will ship to Creditor, upon Creditor's election, the Products repossessed and Creditor will have the option, but not the obligation, to purchase such Products including without limitation, right of offset.
Conditions and terms of repurchase:
 1. Creditor shall have the option, but not the obligation, to repurchase as a means of offset, all or any portion of that Product which may be repossessed by Guarantor, including repossessed Product which is in transit to Debtor.
 2. The Price which Creditor agrees to pay to Guarantor will be an amount equal to eighty percent (80%) of Creditor's transaction sale price to Debtor (Guarantor shall pay freight charge and insurance premium for the reshipment of the acceptable Product to Creditor).
 3. The failure of Guarantor or Creditor to exercise any rights granted hereunder shall not operate as a waiver of those rights.
19. Guarantor may not assign or transfer to sell its rights under this Agreement (or delegate its obligations hereunder) without the prior written consent of Creditor. Creditor may assign this agreement to a parent, subsidiary of affiliated firm or to another entity in connection with the sale or transfer of all or substantially all of its business assets. Subject to these restrictions, the provisions of this Agreement shall be binding upon and shall inure to the benefit of the parties of their permitted assigns.
20. Creditor may terminate this Agreement at any time effective upon written notice to Guarantor, but the termination shall in no manner terminate the Guarantor's liability with respect to financial transactions entered into by Guarantor or Creditor with Debtor prior to the effective date of termination, including without limitation, transactions which will not be completed until after the effective date of termination. Debtor may terminate this Agreement by sending a notice of revocation by registered mail address to the Creditor at: Directed Electronics, Inc., 2560 Progress Street, Vista, California 92083, Attention Credit Manager. Such revocation shall not affect any of the Guarantor's obligations hereunder with respect to indebtedness theretofore incurred nor shall it affect any obligation of any other guarantor of the Debtors obligation to the Creditor.

Automate Authorization:

1. Definitions

- 1.01 Car Dealer. Throughout this addendum the term "Car Dealer" shall refer to any person or entity that resells never-before registered (brand new) motor vehicles to the general public. This facility must be licensed by both the state in which it resides and by the Department of Revenue Services as well as be registered with the Department of Motor Vehicles. A dealer selling only pre-owned vehicles does not classify as a Car Dealer in this Agreement.

2. Program Purpose

- 2.01 Appointment of Authorized Dealer. The above mentioned Dealer requests consideration to become an Authorized AUTOMATE Dealer. The Dealer is presently an Authorized DEI Dealer, has received a copy of the "Authorized Dealer Agreement", has read it, understands it, and shall be bound by all of the terms, conditions, duties and obligations thereof.

3. Authorized Dealer's Functions

- 3.01 DEI hereby authorizes the Dealer to resell AUTOMATE products to the Car Dealer. This right pertains to selling only the AUTOMATE product line and only to the Car Dealer, it does not in any way authorize the Dealer to resell, trade or tranship any other DEI product to any other person or entity for the purpose of resale.
- 3.02 Authorized dealer hereby agrees not to resell, trade or tranship AUTOMATE products to any retail customer or any other person or entity other than a Car Dealer.

4. Advertising

- 4.01 Authorized Dealer agrees not to advertise or engage in any promotional activities concerning AUTOMATE products unless:
 - A. The advertisement or promotion is strictly designed only to benefit the Car Dealer.
 - B. The advertisement or promotion makes no mention of who the AUTOMATE Authorized Dealer is.

5. Term and Termination

- 5.01 This addendum incorporates by reference all the terms, conditions, rights, duties and obligations of the "Authorized Dealer Agreement" and also is contemporaneous with and will expire along with the original "Authorized Dealer Agreement".
- 5.02 This addendum is subject to approval and acceptance by DEI.
- 5.03 This addendum can be terminated for any of the reasons mentioned in Article 6 of the "Authorized Dealer Agreement" including, without limitation, with or without cause.

Neon Sign Authorization:

The Authorized Dealer shall properly maintain and exhibit these Neon Signs and their contents. Any changes or alterations, to these Neon Display(s), by the Authorized Dealer, shall first be approved by a DEI Regional Sales Manager (in writing) prior to the modification being made.

DEI reserves the right to recall any and all Neon Signs from the Authorized Dealer, at any time, for any reason whatsoever and without any notice or cause and the Authorized Dealer agrees to return the Neon Signs to DEI, without delay.

If the Neon Signs are recalled within one (1) year of purchase, DEI will refund 50% of the purchase price. If the signs are recalled within two (2) years of purchase, DEI will refund 20% of the purchase price. If the neon signs are recalled after two years of purchase, DEI will refund 1% of the purchase price.

Authorized Dealer shall pay a sum of \$1,000.00 per Neon Sign to DEI in the event that the Authorized Dealer is unable to return the Neon Sign(s) to DEI, for any reason whatsoever, without regard to fault or offset, provided DEI requests that said Neon Sign(s) be returned.

Authorized Dealer-Employee Purchase Program:

We would like all of our Authorized Dealers and their employees to have the best in security on their personal vehicles. To make this affordable for everyone, we are providing our employee purchase accommodation program. Once a year (one time per calendar year), any employee may purchase products from any DEI line for which you are an Authorized Dealer, along with accessories at 25% off the base price.

The only requirements are that the systems must be professionally installed on the employee's own personal vehicle. The attached purchase form must be completely filled out and signed by the DEI Sales Rep, and the order must be submitted with payment in advance, credit card, money order or certified check only. An employee owning more than one vehicle can make a special request for additional systems. Due to the discount you receive from the employee purchase, DEI's Guaranteed Protection Plan (GPP) does NOT apply.

Explanation of DEI's Guaranteed Protection Plan (GPP):

Directed Electronics, Inc. (DEI) will refund the amount of the comprehensive insurance deductible (not to exceed \$2500.00) to the original owner of an automobile (Motorcycles are not covered) which is stolen while equipped with one of DEI's qualifying security systems provided the following conditions are met:

- A. The qualifying system was sold, installed, and serviced by an Authorized Dealer for DEI, remains in the car in which the system was originally installed, and owned by the original purchaser of the qualifying system. Window decals must have been in place on the vehicle at the time of theft
- B. The theft occurred less than one year after the date of purchase of the qualifying DEI system.
- C. This GPP claim is made within ninety (90) days of settlement of the customer's claim with their insurance carrier.
- D. The warranty registration card was completely filled out and mailed 10 days of purchase.
- E. The vehicle was stolen as a result of alarm system failure and the automobile was not left in an inactive/disarmed mode for whatever reason, even if left at a service station.
- F. A police report must be filed and a copy submitted with the GPP claim. (Note: New York City and surrounding cities must submit the "Verification of Crime/Last Property Report" in place of a general police report.)
- G. Vehicle must be insured against theft at the time vehicle was stolen. (comprehensive coverage)
- H. The insurance company must accept and pay the claim.
- I. A DEI starter kill device must have been installed on the vehicle and both the sales receipt and warranty card must show starter kill installation.

All of the criteria as stated above must be met in order to file a claim for reimbursement of the comprehensive deductible.

IMPORTANT NOTE: A product's warranty is automatically void if its date code or serial number is defaced, missing, or altered. GPP does not cover vandalism; theft of vehicle parts, or its contents; damage to vehicle and/or towing charges. Furthermore, vehicles that are consigned or displayed for sale are not covered by the GPP program. GPP is not available to employees, agents, friends or relatives of DEI or of its Authorized Dealers. GPP does not extend to or cover motorcycles or vehicles without lockable doors, ignition systems and/or engine compartments.

All questions regarding GPP should be directed to DEI customer service. The customer will be provided with complete instructions upon filing a claim, including a list of the necessary documents. It is the responsibility of the customer, not the Authorized Dealer, to obtain and provide the necessary documentation for filing a claim.

The claimant is reminded that in consideration of this program and as a condition precedent to the purchase of the DEI security system, the purchaser agrees (agreed) that any and all claims and/or disputes between the purchaser and DEI shall be decided in accordance with the laws of the State of California and the exclusive and only venue for the same shall be California State Courts in the County of San Diego, California.

Terms and Conditions for Authorized Dealers, Summary

Consumer Limited Lifetime Warranty

For a period of one calendar year from the date of purchase of this auto security device, Directed Electronics, Inc. promises to the ORIGINAL PURCHASER to repair or replace (with a comparable reconditioned model), free of cost, any electronic control module which proves to be defective in workmanship or material under normal use, SO LONG AS THE SYSTEM WAS SOLD, INSTALLED, AND SERVICED BY A PROFESSIONAL AUTO INSTALLER, AND REMAINS IN THE CAR IN WHICH THE SYSTEM WAS ORIGINALLY INSTALLED. If warranty service is necessary you must have a clear copy of your sales receipt containing all of the information shown on the following page.

After the first calendar year, from the date of purchase of this auto security device, Directed Electronics, Inc., promises to the ORIGINAL PURCHASER to repair or replace (with a comparable reconditioned model) any electronic control module which proves to be defective in workmanship or material under normal use FOR A CHARGE OF \$45.00, SO LONG AS THE SYSTEM WAS SOLD, INSTALLED, AND SERVICED BY A PROFESSIONAL AUTO INSTALLER, AND REMAINS IN THE CAR IN WHICH THE SYSTEM WAS ORIGINALLY INSTALLED. If warranty service is necessary you must have a clear copy of your sales receipt containing all of the information shown on the following page.

This warranty contains the entire agreement relating to warranty and supersedes all previous and contemporaneous representations or understandings, whether written or oral. IN ANY EVENT, DEI IS NOT LIABLE FOR THE THEFT OF THE VEHICLE AND/OR ITS CONTENTS OR ANY DAMAGE TO THE VEHICLE AS A RESULT OF A THEFT OR ATTEMPTED THEFT.

This warranty is void if the product has been damaged by accident, unreasonable use, neglect, improper service or other causes not arising out of defects in materials or construction. This warranty is nontransferable and does not apply to any unit that has been modified or used in a manner contrary to its intended purpose and does not cover batteries. The unit in question must be returned to the manufacturer, postage prepaid. This warranty does not cover labor costs for the removal, diagnosis, troubleshooting or reinstallation of the unit. For service on an out-of-warranty product a flat rate fee by model is charged. Contact your authorized dealer to obtain the service charge for your unit.

These systems are a deterrent against possible theft. Directed Electronics, Inc. is not offering a guarantee or insurance against the theft of the automobile or its contents and disclaims any liability for the theft of the vehicle and/or its contents. Directed Electronics does not authorize any person to create for it any other obligation or liability in connection with this security system.

Consumer Limited Lifetime Warranty

Directed Electronics, Inc. ("DEI") promises to the original purchaser to repair or replace with a comparable reconditioned model any DEI® unit (hereafter the "unit"), excluding without limitation the siren, the remote transmitters, the associated sensors and accessories, which proves to be defective in workmanship or material under reasonable use during the lifetime of the vehicle provided the following conditions are met: the unit was professionally installed and serviced by an authorized DEI dealer; the unit will be professionally reinstalled in the vehicle in which it was originally installed by an authorized DEI dealer; and the unit is returned to DEI, shipping prepaid with a legible copy of the bill of sale or other dated proof of purchase bearing the following information: consumer's name, telephone number and address; the authorized dealers name, telephone number and address; complete product description, including accessories; the year, make and model of the vehicle; vehicle license number and vehicle identification number. All components other than the unit, including without limitation the siren, the remote transmitters and the associated sensors and accessories, carry a one-year warranty from the date of purchase of the same. This warranty is non-transferable and is automatically void if: the original purchaser has not completed the warranty card and mailed it within ten (10) days of the date of purchase to the address listed on the card; the unit's date code or serial number is defaced, missing or altered; the unit has been modified or used in a manner contrary to its intended purpose; the unit has been damaged by accident, unreasonable use, neglect, improper service, installation or other causes not arising out of defects in materials or construction. The warranty does not cover damage to the unit caused by installation or removal of the unit. DEI, in its sole discretion, will determine what constitutes excessive damage and may refuse the return of any unit with excessive damage. TO THE MAXIMUM EXTENT ALLOWED BY LAW, ALL WARRANTIES, INCLUDING BUT NOT LIMITED TO EXPRESS WARRANTY, IMPLIED WARRANTY, WARRANTY OF MERCHANTABILITY, FITNESS FOR PARTICULAR PURPOSE AND WARRANTY OF NON-INFRINGEMENT OF INTELLECTUAL PROPERTY, ARE EXPRESSLY EXCLUDED; AND DEI NEITHER ASSUMES NOR AUTHORIZES ANY PERSON OR ENTITY TO ASSUME FOR IT ANY DUTY, OBLIGATION OR LIABILITY IN CONNECTION WITH ITS PRODUCTS. DEI DISCLAIMS AND HAS ABSOLUTELY NO LIABILITY FOR ANY AND ALL ACTS OF THIRD PARTIES INCLUDING ITS AUTHORIZED DEALERS OR INSTALLERS. DEI SECURITY SYSTEMS, INCLUDING

THIS UNIT, ARE DETERRENTS AGAINST POSSIBLE THEFT. DEI IS NOT OFFERING A GUARANTEE OR INSURANCE AGAINST VANDALISM, DAMAGE OR THEFT OF THE AUTOMOBILE, ITS PARTS OR CONTENTS; AND HEREBY EXPRESSLY DISCLAIMS ANY LIABILITY WHATSOEVER, INCLUDING WITHOUT LIMITATION, LIABILITY FOR THEFT, DAMAGE AND/OR VANDALISM. THIS WARRANTY DOES NOT COVER LABOR COSTS FOR MAINTENANCE, REMOVAL OR REINSTALLATION OF THE UNIT OR ANY CONSEQUENTIAL DAMAGES OF ANY KIND. IN THE EVENT OF A CLAIM OR A DISPUTE INVOLVING DEI OR ITS SUBSIDIARY, THE PROPER VENUE SHALL BE SAN DIEGO COUNTY IN THE STATE OF CALIFORNIA. CALIFORNIA STATE LAWS AND APPLICABLE FEDERAL LAWS SHALL APPLY AND GOVERN THE DISPUTE. THE MAXIMUM RECOVERY UNDER ANY CLAIM AGAINST DEI SHALL BE STRICTLY LIMITED TO THE AUTHORIZED DEI DEALER'S PURCHASE PRICE OF THE UNIT. DEI SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO, ANY CONSEQUENTIAL DAMAGES, INCIDENTAL DAMAGES, DAMAGES FOR THE LOSS OF TIME, LOSS OF EARNINGS, COMMERCIAL LOSS, LOSS OF ECONOMIC OPPORTUNITY AND THE LIKE. NOTWITHSTANDING THE ABOVE, THE MANUFACTURER DOES OFFER A LIMITED WARRANTY TO REPLACE OR REPAIR THE CONTROL MODULE AS DESCRIBED ABOVE. Some states do not allow limitations on how long an implied warranty will last or the exclusion or limitation of incidental or consequential damages. This warranty gives you specific legal rights and you may also have other rights that vary from State to State. This product may be covered by a Guaranteed Protection Plan ("GPP"). See your authorized DEI dealer for details of the plan or call DEI Customer Service at 1-800-876-0800. DEI security systems, including this unit, are deterrents against possible theft. DEI is not offering a guarantee or insurance against vandalism, damage or theft of the automobile, its parts or contents; and hereby expressly disclaims any liability whatsoever, including without limitation, liability for theft, damage and/or vandalism. DEI does not and has not authorized any person or entity to create for it any other obligation, promise, duty or obligation in connection with this security system.

Warranty Plus Program

Exclusively for Active Authorized Dealers Only

For 24 months from the product's date code. Directed Electronics, Inc. promises to the active Authorized Dealer to replace any electronic control module that proves to be defective in workmanship or material under normal use. During this 24-month period, there will be no charge for this replacement with new product.

Trade-In. For the period of 25 to 60 months from the product's date code, DEI will offer the active Authorized Dealer new product at a discount of 50 percent off the Authorized Dealer's normal cost as a replacement.

If the product's date code is within 25 - 60 months, and the Authorized Dealer prefers not to take advantage of the Trade-In program, there will be no charge for reconditioned product as replacement. After 6- months from the product's date code, the warranty reverts to the consumer warranty shown above. There will be no charge for comparable reconditioned product so long as the system was installed and is serviced by an Authorized Dealer and remains in the car in which the system is originally installed. The product must also include a copy of the original purchase receipt from the consumer bearing the following information:

Date of purchase, consumer's name and address, Authorized Dealer's name and address, the type of product installed, the year, make and model of the automobile, automobile license number, vehicle identification number and all of the security options installed on the automobile at the time of purchase.

Please refer to the Warranty Plus packing list for more information.

TO: Commissioner of Patents and Trademarks Washington, D.C. 20231	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT
--	--

In compliance with the Act of July 19, 1952 (66 Stat. 814; 35 U.S.C. 290) you are hereby advised that a court action has been filed on the following patent(s) in the U.S. District Court:

DOCKET NO. 02-CV-1727 JM(JAH)	DATE FILED 08-29-02	U.S. DISTRICT COURT United States District Court, Southern District of California
PLAINTIFF Directed Electronics, Inc.		DEFENDANT Steve Dahlin, dba The Lone Gunmen
PATENT NO.	DATE OF PATENT	PATENTEE
1 1,674,046	02-04-92	Clifford Electronics, Inc.
2 1,822,606	02-22-94	Directed Electronics, Inc.
3 1,756,693	03-09-93	Directed Electronics, Inc.
4 1,822,608	02-22-94	Directed Electronics, Inc.
5 1,873,747	01-17-95	Directed Electronics, Inc.

In the above-entitled case, the following patent(s) have been included:

DATE INCLUDED	INCLUDED BY <input type="checkbox"/> Amendment <input type="checkbox"/> Answer <input type="checkbox"/> Cross Bill <input type="checkbox"/> Other Pleading			
PATENT NO.	DATE OF PATENT	PATENTEE		
1				
2				
3				
4				
5				

In the above-entitled case, the following decision has been rendered or judgment issued:

DECISION/JUDGMENT		
CLERK	(BY) DEPUTY CLERK	DATE

Copy 1 - Upon initiation of action, mail this copy to Commissioner Copy 3 - Upon termination of action, mail this copy to Commissioner
 Copy 2 - Upon filing document adding patent(s), mail this copy to Commissioner Copy 4 - Case file copy

PATENT NO.	DATE OF PATENT	PATENTEE
6. 2,218,082	01-19-99	Directed Electronics, Inc.
7. 1,848,176	08-02-94	Directed Electronics, Inc.
8. 4,887,064	12-12-89	Clifford Electronics, Inc.
9. 5,157,375	10-20-92	Clifford Electronics, Inc.
10. 5,534,845	07-09-96	Clifford Electronics, Inc.
11. 5,646,591	07-08-97	Directed Electronics, Inc.
12. Des.345,711	04-05-94	Directed Electronics, Inc.
13. 4,584,569	04-22-86	Directed Electronics, Inc.
14. 5,532,670	07-02-96	Directed Electronics, Inc.

AO 120 (3/85)

TO: Commissioner of Patents and Trademarks Washington, D.C. 20231	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT
--	--

In compliance with the Act of July 19, 1952 (66 Stat. 814; 35 U.S.C. 290) you are hereby advised that a court action has been filed on the following patent(s) in the U.S. District Court:

DOCKET NO. 02-CV-1727 JM(JAH)	DATE FILED 08-29-02	U.S. DISTRICT COURT United States District Court, Southern District of California
PLAINTIFF Directed Electronics, Inc.		DEFENDANT Steve Dahlin, dba The Lone Gunmen
PATENT NO.	DATE OF PATENT	PATENTEE
1 1,674,046	02-04-92	Clifford Electronics, Inc.
2 1,822,606	02-22-94	Directed Electronics, Inc.
3 1,756,693	03-09-93	Directed Electronics, Inc.
4 1,822,608	02-22-94	Directed Electronics, Inc.
5 1,873,747	01-17-95	Directed Electronics, Inc.

In the above-entitled case, the following patent(s) have been included:

DATE INCLUDED	INCLUDED BY <input type="checkbox"/> Amendment <input type="checkbox"/> Answer <input type="checkbox"/> Cross Bill <input type="checkbox"/> Other Pleading			
PATENT NO.	DATE OF PATENT	PATENTEE		
1				
2				
3				
4				
5				

In the above-entitled case, the following decision has been rendered or judgment issued:

DECISION/JUDGMENT		
CLERK	(BY) DEPUTY CLERK	DATE

Copy 1 - Upon initiation of action, mail this copy to Commissioner Copy 3 - Upon termination of action, mail this copy to Commissioner
 Copy 2 - Upon filing document adding patent(s), mail this copy to Commissioner Copy 4 - Case file copy

PATENT NO.	DATE OF PATENT	PATENTEE
6. 2,218,082	01-19-99	Directed Electronics, Inc.
7. 1,848,176	08-02-94	Directed Electronics, Inc.
8. 4,887,064	12-12-89	Clifford Electronics, Inc.
9. 5,157,375.	10-20-92	Clifford Electronics, Inc.
10. 5,534,845	07-09-96	Clifford Electronics, Inc.
11. 5,646,591	07-08-97	Directed Electronics, Inc.
12. Des.345,711	04-05-94	Directed Electronics, Inc.
13. 4,584,569	04-22-86	Directed Electronics, Inc.
14. 5,532,670	07-02-96	Directed Electronics, Inc.

TO: Commissioner of Patents and Trademarks Washington, D.C. 20231	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT
--	--

In compliance with the Act of July 19, 1952 (66 Stat. 814; 35 U.S.C. 290) you are hereby advised that a court action has been filed on the following patent(s) in the U.S. District Court:

DOCKET NO. 02-CV-1727 JM(JAH)	DATE FILED 08-29-02	U.S. DISTRICT COURT United States District Court, Southern District of California
PLAINTIFF Directed Electronics, Inc.		DEFENDANT Steve Dahlin, dba The Lone Gunmen
PATENT NO.	DATE OF PATENT	PATENTEE
1 1,674,046	02-04-92	Clifford Electronics, Inc.
2 1,822,606	02-22-94	Directed Electronics, Inc.
3 1,756,693	03-09-93	Directed Electronics, Inc.
4 1,822,608	02-22-94	Directed Electronics, Inc.
5 1,873,747	01-17-95	Directed Electronics, Inc.

In the above-entitled case, the following patent(s) have been included:

DATE INCLUDED	INCLUDED BY <input type="checkbox"/> Amendment <input type="checkbox"/> Answer <input type="checkbox"/> Cross Bill <input type="checkbox"/> Other Pleading			
PATENT NO.	DATE OF PATENT	PATENTEE		
1				
2				
3				
4				
5				

In the above-entitled case, the following decision has been rendered or judgment issued:

DECISION/JUDGMENT		
CLERK	(BY) DEPUTY CLERK	DATE

Copy 1 - Upon initiation of action, mail this copy to Commissioner Copy 3 - Upon termination of action, mail this copy to Commissioner
 Copy 2 - Upon filing document adding patent(s), mail this copy to Commissioner Copy 4 - Case file copy

PATENT NO.	DATE OF PATENT	PATENTEE
6. 2,218,082	01-19-99	Directed Electronics, Inc.
7. 1,848,176	08-02-94	Directed Electronics, Inc.
8. 4,887,064	12-12-89	Clifford Electronics, Inc.
9. 5,157,375	10-20-92	Clifford Electronics, Inc.
10. 5,534,845	07-09-96	Clifford Electronics, Inc.
11. 5,646,591	07-08-97	Directed Electronics, Inc.
12. Des.345,711	04-05-94	Directed Electronics, Inc.
13. 4,584,569	04-22-86	Directed Electronics, Inc.
14. 5,532,670	07-02-96	Directed Electronics, Inc.

JS44

(Rev. 07/89)

CIVIL COVER SHEET

FILED

The JS-44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON THE SECOND PAGE OF THIS FORM.)

I (a) PLAINTIFFS

DIRECTED ELECTRONICS, INC., a California corporation

DEFENDANTS **02 AUG 29 PM 1:48**
 STEVE DAHLIN, an individual doing business as THE LONE GUNMEN
 DISTRICT COURT
 COUNTY OF CALIFORNIA

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF San Diego
 (EXCEPT IN U.S. PLAINTIFF CASES)

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT
 (IN U.S. PLAINTIFF CASES ONLY) EPITV

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED

(c) ATTORNEYS (FIRM NAME, ADDRESS, AND TELEPHONE NUMBER)

Kristen E. Caverly
 HENDERSON & CAVERLY LLP
 P.O. Box 9144
 Rancho Santa Fe, CA 92067

ATTORNEYS (IF KNOWN)

'02 CV 1727 JM (JAH)

II. BASIS OF JURISDICTION (PLACE AN X IN ONE BOX ONLY)

- 1 U.S. Government Plaintiff
- 3 Federal Question (U.S. Government Not a Party)
- 2 U.S. Government Defendant
- 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (PLACE AN X IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT)

- | | | | |
|---|---|---|---|
| (For Diversity Cases Only) | | PT DEF | PT DEF |
| Citizen of This State | <input type="checkbox"/> 1 <input type="checkbox"/> 1 | Incorporated or Principal Place of Business in This State | <input type="checkbox"/> 4 <input type="checkbox"/> 4 |
| Citizen of Another State | <input type="checkbox"/> 2 <input type="checkbox"/> 2 | Incorporated and Principal Place of Business in Another State | <input type="checkbox"/> 5 <input type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 <input type="checkbox"/> 3 | Foreign Nation | <input type="checkbox"/> 6 <input type="checkbox"/> 6 |

IV. CAUSE OF ACTION (CITE THE US CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE. DO NOT CITE JURISDICTIONAL STATUTES UNLESS DIVERSITY.)

Patent Infringement (35 U.S.C. Section 271); Trademark Infringement (15 U.S.C. Section 1114)

V. NATURE OF SUIT (PLACE AN X IN ONE BOX ONLY)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
<input type="checkbox"/> 110 Insurance	PERSONAL INJURY	<input type="checkbox"/> 610 Agriculture	<input type="checkbox"/> 422 Appeal 28 USC 158	<input type="checkbox"/> 400 State Reappointment
<input type="checkbox"/> 120 Marine	<input type="checkbox"/> 310 Airplane	<input type="checkbox"/> 620 Other Food & Drug	<input type="checkbox"/> 423 Withdrawal 28 USC 157	<input type="checkbox"/> 410 Antitrust
<input type="checkbox"/> 130 Miller Act	<input type="checkbox"/> 315 Airplane Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881	PROPERTY RIGHTS	<input type="checkbox"/> 430 Banks and Banking
<input type="checkbox"/> 140 Negotiable Instrument	<input type="checkbox"/> 320 Assault, Libel & Slander	<input type="checkbox"/> 630 Liquor Laws	<input type="checkbox"/> 820 Copyrights	<input type="checkbox"/> 450 Commerce/ICC Rates/etc.
<input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment	<input type="checkbox"/> 330 Federal Employers' Liability	<input type="checkbox"/> 640 RR & Truck	<input checked="" type="checkbox"/> 830 Patent	<input type="checkbox"/> 460 Deportation
<input type="checkbox"/> 151 Medicare Act	<input type="checkbox"/> 340 Marine	<input type="checkbox"/> 650 Airline Regs	TRADEMARK	<input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations
<input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excl. Veterans)	<input type="checkbox"/> 345 Marine Product Liability	<input type="checkbox"/> 660 Occupational Safety/Health	SOCIAL SECURITY	<input type="checkbox"/> 810 Selective Service
<input type="checkbox"/> 153 Recovery of Overpayment of Veterans Benefits	<input type="checkbox"/> 350 Motor Vehicle	<input type="checkbox"/> 690 Other	<input type="checkbox"/> 861 HIA (13958)	<input type="checkbox"/> 850 Securities/Commodities Exchange
<input type="checkbox"/> 160 Stockholders Suits	<input type="checkbox"/> 355 Motor Vehicle Product Liability	LABOR	<input type="checkbox"/> 862 Black Lung (923)	<input type="checkbox"/> 875 Customer Challenge 12 USC
<input type="checkbox"/> 190 Other Contract	<input type="checkbox"/> 360 Other Personal Injury	<input type="checkbox"/> 710 Fair Labor Standards Act	<input type="checkbox"/> 863 DIWC/DIWW (405(g))	<input type="checkbox"/> 891 Agricultural Acts
<input type="checkbox"/> 195 Contract Product Liability		<input type="checkbox"/> 720 Labor/Mgmt. Relations	<input type="checkbox"/> 864 SSID Title XVI	<input type="checkbox"/> 892 Economic Stabilization Act
		<input type="checkbox"/> 730 Labor/Mgmt. Reporting & Disclosure Act	<input type="checkbox"/> 865 RSI (405(e))	<input type="checkbox"/> 893 Environmental Matters
		<input type="checkbox"/> 740 Railway Labor Act	FEDERAL TAX SUITS	<input type="checkbox"/> 894 Energy Allocation Act
REAL PROPERTY	CIVIL RIGHTS	<input type="checkbox"/> 790 Other Labor Litigation	<input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant)	<input type="checkbox"/> 895 Freedom of Information Act
<input type="checkbox"/> 210 Land Condemnation	<input type="checkbox"/> 441 Voting	<input type="checkbox"/> 791 Empl. Ret. Inc. Security Act	<input type="checkbox"/> 871 IRS - Third Party 26 USC 7609	<input type="checkbox"/> 900 Appeal of Fee Determination Under Equil Access to Justice
<input type="checkbox"/> 220 Foreclosure	<input type="checkbox"/> 442 Employment			<input type="checkbox"/> 950 Constitutionality of State
<input type="checkbox"/> 230 Rent Lease & Eiectmant	<input type="checkbox"/> 443 Housing/Accommodations			<input type="checkbox"/> 890 Other Statutory Actions
<input type="checkbox"/> 240 Tort to Land	<input type="checkbox"/> 444 Welfare			
<input type="checkbox"/> 245 Tort Product Liability	<input type="checkbox"/> 440 Other Civil Rights			
<input type="checkbox"/> 290 All Other Real Property				
	PRISONER PETITIONS			
	<input type="checkbox"/> 510 Motions to Vacate Sentence Habeas Corpus			
	<input type="checkbox"/> 530 General			
	<input type="checkbox"/> 535 Death Penalty			
	<input type="checkbox"/> 540 Mandamus & Other			
	<input type="checkbox"/> 550 Civil Rights			
	<input type="checkbox"/> 555 Prisoner Conditions			

VI. ORIGIN (PLACE AN X IN ONE BOX ONLY)

- 1 Original Proceeding
- 2 Removal from State Court
- 3 Remanded from Appellate Court
- 4 Reinstated or Reopened
- 5 Transferred from another district (specify)
- 6 Multidistrict Litigation
- 7 Appeal to District Judge from Magistrate Judgment

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER f.r.c.p. 23

DEMAND \$ more than \$100,000

Check YES only if demanded in complaint:
 JURY DEMAND YES NO

VIII. RELATED CASE(S) IF ANY (See Instructions):

JUDGE See Notice of Related Cases

Docket Number

DATE August 28, 2002

SIGNATURE OF ATTORNEY OF RECORD Kristen E. Caverly

Handwritten: \$150.00 8/29/02 #86108 RD