UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ROKU, INC.,
Petitioner,

v.

ECOLINK INTELLIGENT TECHNOLOGY, INC.,
Patent Owner.

Case IPR2023-00792

U.S. Patent No. 10,692,340

DECLARATION OF BRUCE MCNAIR IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 10,692,340

TABLE OF CONTENTS

Page

I. INTRODUCTION 1
A. Engagement 1
B. Background and Qualifications 2
C. Basis of My Opinion and Materials Considered 5
D. Legal Standards for Patentability 6
1. Obviousness 6
2. Claim Construction 10
II. BACKGROUND OF THE TECHNOLOGY 12
III. THE '340 PATENT 14
A. '340 Patent Overview 14
B. Prosecution History of the '340 Patent 16
IV. THE '340 PATENT PRIORITY DATE 18
V. LEVEL OF ORDINARY SKILL IN THE ART 19
VI. CLAIM CONSTRUCTION 20
VII. GROUNDS OF UNPATENTABILITY 21
A. Ground 1: Lamb in view of Williams (Claims 1-2, 6, 11-12, and 16) 22
1. U.S. Patent Application Publication No. 2016/0247370 ("Lamb") Overview 22
2. U.S. 6,057,764 ("Williams") Overview and Motivation to Combine with Lamb 25
3. Invalidity of Claims 1-2, 6, 11-12, and 16 Over Lamb in view of Williams 30
(a) Element [1.pre] 30
(b) Element [1.a] 32

(c) Element [1.b] 34
(d) Element [1.c] 36
(e) Element [1.d] 45
(f) Element [1.e] 46
(g) Element [1.f] 49
(h) Element [1.g] 51
(i) Claim [2] 59
(j) Element [6.pre] 62
(k) Element [6.a] 63
(l) Element [6.b] 66
(m) Element [6.c] 68
(n) Element [6.d] 69
(o) Element [6.e] 70
(p) Element [6.f] 71
(q) Element [6.g] 79
(r) Element [6.h] 81
(s) Element [6.i] 82
(t) Element [11.pre] 83
(u) Element [11.a] 84
(v) Element [11.b] 87
(w) Claim [12] 93
(x) Element [16.pre] 96
(y) Element [16.a] 97
(z) Element [16.b] 98
(aa) Element [16.c] 100
(bb) Element [16.d] 104
(cc) Element [16.e] 106
(dd) Element [16.f] 107

B. Ground 2: Sharma (Claims 1 and 11) 108

1. U.S. 7,696,873 (“Sharma”) Overview 108

2. Invalidity of Claims 1 and 11 Over Sharma 111
(a) Element [1.pre] 111
(b) Element [1.a] 114
(c) Element [1.b] 116
(d) Element [1.c] 119
(e) Element [1.d] 124
(f) Element [1.e] 126

(g) Element [1.f] 128
(h) Element [1.g] 130
(i) Element [11.pre] 132
(j) Element [11.a] 133
(k) Element [11.b] 135

VIII. SECONDARY CONSIDERATIONS 137

IX. CONCLUSION 138

I, Bruce McNair, declare as follows:

I. INTRODUCTION

1. My name is Bruce McNair. I am over the age of eighteen and am competent to make this Declaration.

A. Engagement

2. I have been retained by Roku, Inc. ("Roku" or "Petitioner") to provide my opinions on certain issues related to U.S. Patent No. 10,692,340 (the "'340 patent," which I understand has been designated as Exhibit 1001) in connection with the above-captioned *inter partes* review (IPR) proceeding. In particular, I have been asked to provide my insights, analysis, and opinions regarding whether claims 1-2, 6, 11-12, and 16 of the '340 patent ("Challenged Claims") are obvious over the prior art references identified below.

3. I submit this report on behalf of Roku in connection with its request for *inter partes* review of the '340 patent—to review and to provide my opinion on the scope and content of "prior art" predating the application for the '340 patent and regarding the subject matter recited in the claims of the '340 patent. I understand that this Declaration relates to a petition for the above-captioned *inter partes* review (IPR) of the '340 patent.

4. For my efforts in connection with the preparation of this declaration, I have been compensated at my standard hourly consulting rate. My compensation is

in no way contingent on the results of these or any other proceedings relating to the above-captioned patent. I have no expectation or promise of additional business with the petitioner in exchange for the positions explained herein.

5. I make this declaration based on personal knowledge.

B. Background and Qualifications

6. A detailed description of my professional qualifications, including a listing of my specialties/expertise and professional activities, is contained in my curriculum vitae, a copy of which is attached as Appendix A. In what follows, I provide a short summary of my professional qualifications.

7. I have 60 years of experience in the areas of electronic circuits, starting as an amateur radio operator in 1963 and including seven years as a GS-0855 Electronic Engineer working for the US Army Electronics Command, one year at ITT Defense Communications Division, 24 years as a Member of Technical Staff at AT&T/Bell Laboratories and 15 years as a full-time faculty member of the Electrical and Computer Engineering Department at Stevens Institute of Technology.

8. While I was working for the US Army Electronics Command at Fort Monmouth, NJ, I was responsible for research and development for the data transmission, electronic counter-counter measures (ECCM), and cryptographic aspects of SINCGARS, the Single Channel Ground/Airborne Radio System. As part of this work, I built speech compression hardware and software, microprocessor-

based systems, digital hardware and analog circuits to accomplish my research. I also was responsible for specifying digital transmission equipment and the associated cryptographic equipment. I became familiar with classified military equipment designed to detect and protect against surreptitious physical compromise of the encryption equipment.

9. While I was at ITT Defense Communications Division, I designed digital hardware for a satellite communications system used by the White House. I also designed hardware and software to realize the first hardware implementation of a Linear Predictive Coder, a technology used extensively to this day for speech communications in virtually all communication today.

10. At Bell Labs, I worked on several projects involving public data networks, encryption, analog modems, network security and wireless systems. This included security for an X.25 pre-Internet public data network (Advanced Communications Service/Net-1000). I designed digital hardware and microprocessor-based systems to improve the operation of analog modems. I also initiated and led an IR&D (independent research and development) project to investigate and prototype a secure voice terminal based on newly evolving AT&T high-speed digital services. This involved analog and digital hardware design, microprocessor programming, and controlling systems through a signaling and control network. Part of this work involved interfacing with the analog telephone

network, interfacing with audio input and output devices and digital speech and signal processing. I then led a group developing encryption add-ons for analog modems. As part of this work, I investigated tamper detection circuitry to protect cryptographic equipment from external compromise. Finally, I led the Bell Labs Security Architecture Group, setting security and encryption standards for all AT&T products and services. While I was at Bell Labs, I performed research into future wireless systems, including modulation techniques and voice coding to maximize performance. This involved the design of digital and analog hardware, writing real-time digital signal processing (DSP) software and extensive testing of the system performance.

11. At Stevens Institute of Technology, I have taught undergraduate courses, including Electronic Circuits (EE359) dealing with analog and digital circuits. I was also responsible for the Capstone Senior Design Project in the Electrical and Computer Engineering Department. This project, a two-semester course required of all engineering seniors, requires the investigation, design, and prototyping of a complex electrical or computer system. Besides conducting the course, I was also responsible for directly advising a significant fraction of the projects. I have taught graduate courses (EE584 – Wireless System Security and CpE691 – Information Systems Security) which have heavy emphasis on the application of cryptography, including challenge-response systems and public-key

cryptography. I also taught Physical Design of Wireless Systems (EE585) which deals with the detailed design of wireless systems such as cellular phones and other wireless communications equipment. I also have taught a graduate course, EE517, Digital and Computer Systems Architecture and undergraduate courses, CpE450, Architecture, Design and Implementation of Embedded Systems for Real-Time Applications and CpE-358, Switching Theory and Logical Design, involving microprocessor design and interfacing. After retiring from my full-time teaching position in 2017, I have continued to teach the same graduate courses as part of Stevens on-line program.

12. Based on my work in computer and network security during my career and motivated by my hobbies, I have also employed magnetic sensors/controllers of the type described in the patent for various devices I have designed for my personal use, such as games and puzzles, and I have also designed and installed security, sensor, and alarm systems for my own home.

C. Basis of My Opinion and Materials Considered

13. I have reviewed the ’340 patent and the prior art and other documents and materials cited herein. For ease of reference, the full list of documents that I have considered is included in Appendix B. My opinions in this declaration are based on my review of these documents, as well as upon my education, training, research, knowledge, and experience.

14. I have reviewed, had input into, and endorse as set forth fully herein the discussions in the accompanying petition.

D. Legal Standards for Patentability

15. I am not an attorney and I offer no opinions on the law itself. My understanding of the relevant law principles this section is based on information provided to me by counsel.

1. Obviousness

16. I have been informed that a claim may be unpatentable under 35 U.S.C. § 103(a) if the subject matter described by the claim as a whole would have been obvious in view of a prior art reference or in view of a combination of references at the time the alleged invention was made. I have been informed that obviousness is determined from the perspective of a hypothetical person of ordinary skill in the art ("POSITA" or "person of ordinary skill") and that the challenged claims of the patent should be read from the point of view of such a person at the time the alleged invention was made. I have been informed that a hypothetical person of ordinary skill is assumed to know and to have all relevant prior art in the field of endeavor covered by the patent in suit, and would thus have been familiar with each of the references cited herein, as well as the background knowledge in the art, and the full range of teachings they contain.

17. I have been informed that there are two criteria for determining whether prior art is analogous and thus can be considered prior art: (1) whether the art is from the same field of endeavor, regardless of the problem addressed, and (2) if the reference is not within the field of the patentee's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the patentee is involved. I have also been informed that the field of endeavor of a patent is not limited to the specific point of novelty, the narrowest possible conception of the field, or the particular focus within a given field. I have also been informed that a reference is reasonably pertinent if, even though it may be in a different field from that of the patentee's endeavor, it is one which, because of the matter with which it deals, logically would have commended itself to a patentee's attention in considering his problem.

18. I have also been informed that an analysis of whether an alleged invention would have been obvious should be considered in light of the scope and content of the prior art, the differences (if any) between the prior art and the alleged invention, and the level of ordinary skill in the pertinent art involved. I have been informed as well that a prior art reference should be viewed as a whole.

19. I have also been informed that in considering whether an invention for a claimed combination would have been obvious, I may assess whether there are apparent reasons to combine known elements in the prior art in the manner claimed

in view of interrelated teachings of multiple prior art references, the effects of demands known to the design community or present in the market place, and/or the background knowledge possessed by a person of ordinary skill. I have been informed that other principles may be relied on in evaluating whether an alleged invention would have been obvious, and that these principles include the following:

- A combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results;
- When a device or technology is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or in a different one, so that if a person of ordinary skill can implement a predictable variation, the variation is likely obvious;
- If a technique has been used to improve one device, and a person of ordinary skill would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill;
- An explicit or implicit teaching, suggestion, or motivation to combine two prior art references to form the claimed combination may demonstrate obviousness, but proof of obviousness does not depend on or require showing an explicit teaching, suggestion, or motivation to combine;
- Market demand, rather than scientific literature, can drive design trends and may show obviousness;
- In determining whether the subject matter of a patent claim would have been obvious, neither the particular motivation nor the avowed purpose of the named inventor controls;
- One of the ways in which a patent's subject can be proved obvious is by noting that there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims;
- Any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed;
- "Common sense" teaches that familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle;

- A person of ordinary skill is also a person of ordinary creativity, and is not an automaton;
- A patent claim can be proved obvious by showing that the claimed combination of elements was "obvious to try," particularly when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions such that a person of ordinary skill would have had good reason to pursue the known options within his or her technical grasp; and
- One should be cautious of using hindsight in evaluating whether an alleged invention would have been obvious.

20. I have further been informed that, in making a determination as to whether or not the alleged invention would have been obvious to a person of ordinary skill, the Board may consider certain objective factors if they are present, such as: commercial success of products practicing the alleged invention; long-felt but unsolved need; teaching away; unexpected results; copying; and praise by others in the field. These factors are generally referred to as "secondary considerations" or "objective indicia" of nonobviousness. I have been informed, however, that for such objective evidence to be relevant to the obviousness of a claim, there must be a causal relationship (called a "nexus") between the claim and the evidence and that this nexus must be based on what is claimed and novel in the claim rather than something in the prior art. I also have been informed that even when they are present, secondary considerations may be unable to overcome primary evidence of obviousness (*e.g.*, motivation to combine with predictable results) that is sufficiently strong.

21. I have been asked to consider the patentability of claims 1-2, 6, 11-12, and 16 (the "Challenged Claims") of the '340 patent that are challenged in the Petition. I have been informed that for *inter partes* reviews, unpatentability must be shown under a preponderance of the evidence standard. I have been informed that to establish something by a preponderance of the evidence one needs to prove it is more likely true than not true. I have concluded that the Challenged Claims is unpatentable under 35 U.S.C. § 103 based on Lamb in view of Williams and Sharma as described below, under both the preponderance of the evidence standard as well as the higher standard of clear and convincing evidence.

2. Claim Construction

22. I have been informed that patent claims are construed from the viewpoint of a person of ordinary skill at the time of the alleged invention. I have been informed that patent claims generally should be interpreted consistent with their plain and ordinary meaning as understood by a person of ordinary skill in the relevant time period (*i.e.*, at the time of the purported invention, or the so called "effective filing date" of the patent application), after reviewing the patent claim language, the specification and the prosecution history (*i.e.*, the intrinsic record).

23. I have further been informed that a person of ordinary skill must read the claim terms in the context of the claim itself, as well as in the context of the entire patent specification. I understand that in the specification and prosecution history,

the patentee may specifically define a claim term in a way that differs from the plain and ordinary meaning. I understand that the prosecution history of the patent is a record of the proceedings before the U.S. Patent and Trademark Office, and may contain explicit representations or definitions made during prosecution that affect the scope of the patent claims. I understand that an applicant may, during the course of prosecuting the patent application, limit the scope of the claims to overcome prior art or to overcome an examiner's rejection, by clearly and unambiguously arguing to overcome or distinguish a prior art reference, or to clearly and unambiguously disavow claim coverage.

24. In interpreting the meaning of the claim language, I understand that a person of ordinary skill may also consider "extrinsic" evidence, including expert testimony, inventor testimony, dictionaries, technical treatises, other patents, and scholarly publications. I understand this evidence is considered to ensure that a claim is construed in a way that is consistent with the understanding of a person of ordinary skill in the art at the time of the alleged invention. This can be useful for technical terms whose meaning may differ from its ordinary English meaning. I understand that extrinsic evidence may not be relied on if it contradicts or varies the meaning of claim language provided by the intrinsic evidence, particularly if the applicant has explicitly defined a term in the intrinsic record.

II. BACKGROUND OF THE TECHNOLOGY

25. As discussed in Section III, the purported invention of the ’340 patent is a barrier alarm device used in home and business security applications. Specifically, claim 1, which is representative of the independent claims in the ’340 Patent, and from which other Challenged Claims depend, recites “a barrier alarm device” that includes “a barrier status detection device for indicating that a barrier monitored by the barrier alarm device has been opened” and “a human detection device for indicating that a human being is inside a premises in proximity to the barrier” and uses data from these devices to determine whether or not to “transmit … [a] timed alarm signal.” ’340 patent, Claim 1.

26. Based on my experience in the field, however, the functionalities of the ’340 patent were well-known in the art prior to the ’340 patent’s priority date. One example of such prior art is U.S. Patent Publication No. 2016/0247370 (“Lamb”), which identifies Lamb as its first named inventor. I understand that a copy of Lamb has been designated as Exhibit 1009. Lamb discloses a security system that responds to the same combination of barrier movement and human movement detection sensors in implementing a security system that detects unwanted physical intrusions into a monitored premise. Lamb, [0037], [0040], [0058]-[0059].

27. Another relevant prior art reference is U.S. Patent No. 6,057,764, which identifies Williams as its inventor. I understand that a copy of Williams has been

designated as Exhibit 1010. Williams discloses a security system that generates timed alarm signals in response to signals from a barrier movement detection sensor and a human detection sensor. Williams, 1:64-2:8, 2:66-3:38, 3:49-4:39. As explained in greater detail below in Section VII.A.2, a person having ordinary skill in the art would have been motivated to modify Lamb with Williams's teachings to yield a system that can reliably verify that the detected individual is an authorized occupant of the secured space. Applying Williams's teachings to Lamb yields a system where, upon detection of an open barrier and the subsequent detection of a person within the premises, the system initializes a timer that counts down the period of time within which an authorized individual can verify that they are the person within the premises and disable the alarm that will otherwise be triggered.

28. Yet another prior art reference is U.S. Patent No. 7,696,873, which identifies Sharma as its first named inventor. Sharma discloses a security system that "allows people to move about within [a] perimeter … without generating an alarm" based on sensing the statuses of a door sensing unit and a motion sensor. Sharma, 4:15-21, Fig. 5. Sharma thus discloses a system that reduces false alarms issued by a security system monitoring a premise.

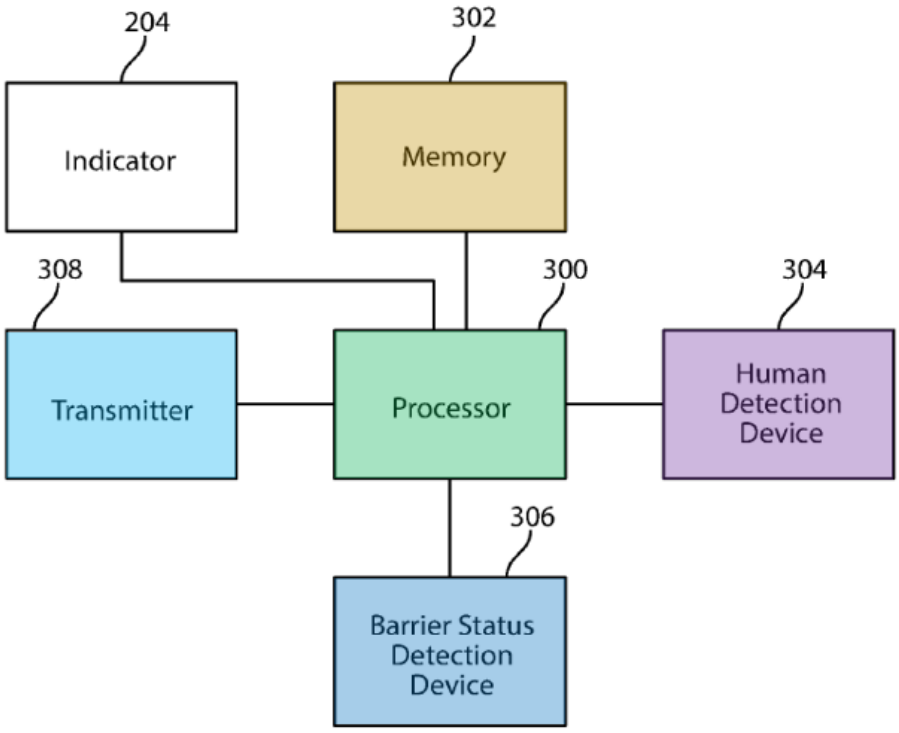
29. None of the features recited in the Challenged Claims of the ’340 patent was novel at the time of the alleged invention, and there was nothing novel as to the manner in which the ’340 patent combined those features.

30. As I discuss below, the Challenged Claims are obvious over the prior art. Further, there were no technological barriers to combining these elements to form the claimed invention and a person having ordinary skill in the art would have been motivated to combine these elements and would have understood that the combination would have yielded predictable results.

III. THE ’340 PATENT

A. ’340 Patent Overview

31. The ’340 patent relates to systems and methods for providing differentiated security responses from a barrier alarm system to reduce the occurrences of false alarms. The ’340 patent discloses a **barrier alarm device 104** that includes a **barrier status detection device 306**, which monitors the status of a **barrier** and determines whether it is open or closed, and a **human detection device 304**, which monitors for the presence of a human within a predetermined distance of the barrier alarm device. ’340, 8:27-31, 8:60-9:2, 9:2-22.



’340 patent, Fig. 3 (annotated).

32. The system responds to status updates from both the **barrier status detection device 306** and the **human detection device 304**. For example, after the **barrier status detection device 306** indicates that a **barrier (i.e., a door/window)** is open, the **barrier alarm device 104’s processor 300** responds by determining via **human detection device 304** whether a person is inside the premises to evaluate the likelihood that the barrier movement was the result of an attempted unauthorized entry. ’340 patent, 9:62-10:6, 15:66-16:20. In the event that both the **barrier status detection device 306** detects that a **door/window** has been opened and the **human detection device 304** detects someone inside the premises, the **processor 300** will transmit a message that causes the **control panel** to initiate a timed alarm signal; this

signal starts with a countdown timer, and upon the expiration of the timer, the system will trigger a security response. ’340, 2:40-48, 4:10-20, 16:54-57. On the other hand, if the **human detection device 304** does not detect someone inside the premises after the **barrier status detection device 306** detects that a **door/window** has been opened, **processor 300** will transmit a message causing the **control panel** to initiate an immediate alarm signal, since this is taken to indicate that the barrier movement “was the result of someone outside the monitored premises attempting unauthorized entry to the premises.” ’340 patent, 4:28-33, 9:65-10:6, 17:35-39. The timed alarm signal is designed to give the authorized user time to cancel the security response, thus reducing the number of false alarms raised by the barrier alarm system. ’340 patent, 4:21-27.

B. Prosecution History of the ’340 Patent

33. In formulating my opinions, I considered the contents of the prosecution history of the ’340 patent, a copy of which I understand has been designated as Exhibit 1002. The ’340 patent issued from U.S. Application No. 16/200,172, filed on November 26, 2018. Ex. 1002, 1, 380.

34. On September 26, 2019, the Examiner issued an Office Action rejecting pending claims 1-20 as obvious over U.S. Patent Application Publication No.

2013/0257611 ("Lamb-611"[1]) in view of U.S. Patent Application Publication No. 2010/0245088 ("Meier").[2] Ex. 1002, 168-172. The Examiner found that the Lamb-611 application taught every limitation of the independent claims except for a "human detection device" that detects when person is inside the relevant premises and in proximity to the barrier. Ex. 1002, 169. However, the Examiner concluded this feature, which was taught by Meier, would have been obvious to incorporate into Lamb-611's device "to accurately detect the presence of a person and/or detecting some movement of an object caused by the person thereby improving the reliability of the system. Ex. 1002, 169.

35. On December 6, 2019, the Applicant responded to this rejection by arguing that the combination of Lamb-611 and Meier does not teach the "cooperative" use of a status indication generated by the barrier alarm device and a status indication generated by a human detection device, such that the system

[1] **Lamb-611** is a different reference from **Lamb** (Ex. 1009), which is used to support the grounds raised in this declaration. Based on my review, I conclude that **Lamb** has a different disclosure from **Lamb-611**.

[2] The Examiner further relied on Ohtsubo (6,542,071), which teaches monitoring for elapsed time and determining whether elapsed time exceeds a predetermined period, to reject pending claims 7-11 and 18-20. EX1002, 171-172.

responds to a signal from the barrier status detection device indicating that a door is open by determining whether a human being is inside the premise using a human detection device. Ex. 1002, 243. The Applicant accordingly amended pending claims 1-3, 7-9, 12-14, and 18-20 to clarify that the human detection device determines whether a human being is inside the premises in proximity to the barrier in response to signals from the barrier status detection device and cancelled pending claims 6 and 17. Ex. 1002, 235-241. The Applicant again amended the pending claims on January 23, 2020 to correct several typographical errors, including the misspelling of the words "indicated" and "to" and the addition of the word "the." Ex. 1002, 251-257.

36. The Examiner allowed the amended claims on February 10, 2020. Ex. 1002, 314-320.

IV. THE '340 PATENT PRIORITY DATE

37. I understand the '340 patent was filed on November 26, 2018 as a continuation-in-part of application No. 15/946,511, filed April 5, 2018, now issued as U.S. Patent No. 10,497,230, which is a division of application No. 14/629,370, filed on February 23, 2015, now issued as U.S. Patent No. 9,940,797. I have not formulated any opinion about the correct priority date for the '340 patent. For purposes of this declaration, I was asked to assume, with respect to each of the prior art Grounds discussed in this declaration, that the '340 patent is entitled to the

priority date of November 26, 2018. I have been instructed to consider the patent and the prior art from the perspective of a person having ordinary skill in the art as of November 26, 2018.

V. LEVEL OF ORDINARY SKILL IN THE ART

38. In rendering the opinions set forth in this declaration, I was asked to consider the patent claims and the prior art through the eyes of a person having ordinary skill in the art at the time of the alleged invention. I understand that the factors considered in determining the ordinary level of skill in a field of art include the level of education and experience of persons working in the field; the types of problems encountered in the field, the teachings of the prior art, and the sophistication of the technology at the time of the alleged invention. I understand that a person having ordinary skill in the art is not a specific real individual, but rather is a hypothetical individual having the qualities reflected by the factors above. I understand that a person having ordinary skill in the art would also have knowledge from the teachings of the prior art, including the art cited below.

39. I have been asked to assume that the ’340 patent is entitled to the priority date of November 26, 2018. Upon consideration of these factors, in my opinion, on or before this priority date, a person of ordinary skill in the art, at the time the application that matured into the ’340 patent was filed, would have had a minimum of a bachelor’s degree in electrical engineering, or a related field, and

approximately two or more years of experience or equivalent study in sensor systems. Additional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education.

40. Well before November 26, 2018, my level of skill in the art was at least that of a person having ordinary skill. I am qualified to opine concerning what a person having ordinary skill in the art would have known and understood at the time of the ’340 patent’s purported invention. My analysis and conclusions herein are from the perspective of a person having ordinary skill in the art as of November 26, 2018. Even if that priority date were earlier, however, my opinions would not change as long as the identified prior art were still prior art.

VI. CLAIM CONSTRUCTION

41. I have been instructed that the Challenged Claims 1-2, 6, 11-12, and 16 of the ’340 patent are to be given their ordinary and customary meaning as understood by one of ordinary skill in the art at the time of the alleged invention in light of the specification and the prosecution history pertaining to the patent, except as provided below. I have followed these principles in my analysis set forth in this document. I reserve the right to supplement my opinions in this declaration to the extent that any parties later propose claim constructions for any claim terms in the ’340 patent.

VII. GROUNDS OF UNPATENTABILITY

42. As I explained above in Section II, the methods for wirelessly reporting sensed conditions claimed in the Challenged Claims were well-known in the art.

43. In this section, I will explain why combinations of teachings from the following references render obvious each of the Challenged Claims:

Name	US Patent/ Publication	Ex.	Priority Date	Filing Date	Published/ Issued
Lamb	U.S. 2016/0247370	1009	2/23/2015	2/23/2015	8/25/2016
Williams	U.S. 6,057,764	1010	8/20/1998	8/20/1998	5/2/2000
Sharma	U.S. 7,696,873	1011	9/12/2006	9/12/2006	4/13/2010

I have been instructed to assume that each of these references qualifies as prior art.

44. As I explain below, the Challenged Claims are invalid based upon the following prior art grounds:

a. **Ground 1:** Challenged Claims 1-2, 6, 11-12, and 16 of the ’340 patent are rendered obvious by Lamb in view of Williams; and

b. **Ground 2:** Challenged Claims 1 and 11 of the ’340 patent are rendered obvious by Sharma.

45. In summary, for **Ground 1**, Lamb teaches a barrier alarm device with several components each configured to perform the same or similar functions as in the ’340 patent, including processor 300 coupled to memory 302, human detection device 304, barrier status detection device 306, and transmitter 308. Lamb, Fig. 3,

[0030]-[0037]. And, in order to explicitly address the timed alarm signal upon detection of an open barrier and human presence within the monitored premises as required in the Challenged Claims, Williams affirmatively discloses such a timed alarm signal within which an authorized user may disable an alarm that would otherwise be triggered. Williams, 3:49-4:39. In **Ground 2**, Sharma discloses a system that includes a door sensing unit that monitors the status of a door (that is, whether the door is open or closed) and a motion detector that monitors for the presence of a human being proximate to the monitored door. Sharma, 4:50-56. In the case where the door sensing unit determines both that the door is open and motion is detected, it may set the system to a "Timed Exit Mode" that temporarily disables the system from making alerts before re-arming the system. Sharma, 7:52-8:18.

46. It is my opinion that Challenged Claims 1-2, 6, 11-12, and 16 of the '340 patent are unpatentable as explained below. I note that in this discussion, I may focus on the particular language in specific claims, but it should be understood that my analysis applies to the corresponding elements of all Challenged Claims containing identical or substantially identical language.

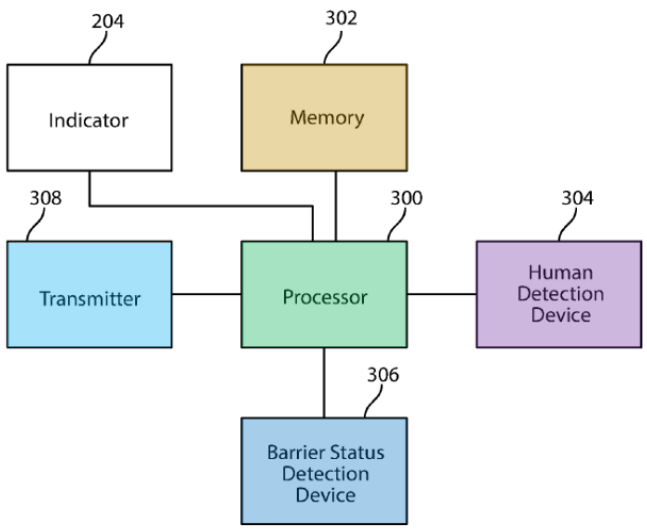
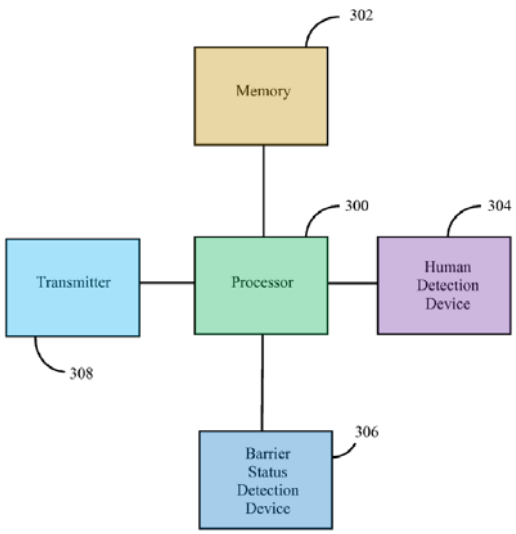
A. Ground 1: Lamb in view of Williams (Claims 1-2, 6, 11-12, and 16)

1. U.S. Patent Application Publication No. 2016/0247370 ("Lamb") Overview

47. **Lamb** is the publication of U.S. Patent Application No. 14/629,370, to which the '340 patent is a continuation-in-part, which I understand to mean that the

’340 patent discloses and/or claims some subject matter disclosed in Lamb and expressly includes disclosures and/or claims that are not in Lamb. After reviewing both Lamb and the ’340 patent, I conclude that Lamb discloses many of the same core features described and claimed in the ’340 patent except for the timing-related disclosures. *See* §III.A.

48. For example, **Lamb** discloses a **barrier alarm device** that is very similar to the **barrier alarm device** disclosed by the ’340 patent and includes many of the same components, such as a **processor 300** coupled to **memory 302**, **human detection device 304**, **barrier status detection device 306**, and **transmitter 308**. Each of these components are configured to perform the same or similar functions in Lamb as they are in the ’340 patent. Lamb, Fig. 3, [0030]-[0037]. To illustrate the high degree of similarity between the ’340 patent’s barrier alarm device and Lamb’s barrier device, see the annotated versions of the respective Figure 3s from the ’340 patent and Lamb below:

'340	**Lamb**
	
Fig. 3	**Fig. 3**

49. **Lamb** also discloses that its system is responsive to indications from both the **barrier status detection device 306** and the **human detection device 304**. For example, Lamb's **processor 300** monitors signals from **barrier status detection device 306** and responds to an indication that a **door** is open by checking to see whether **human detection device 304** "has sensed a person proximate to the barrier alarm device, door or window" who is inside the premises. Lamb, [0037], [0040], [0058]-[0059]. If a human is detected inside the premises proximate to the barrier alarm device or relevant barrier, the system understands this to be an indication "that an authorized person inside the monitored premises has opened the barrier." Lamb, [0040]. Consequently, the **barrier alarm device** transmits a "bypass signal" to the **central security panel 116**, which may direct the **central security panel 116** to, for

example, ignore future alarm signals from the barrier alarm device, disarm the security system, and/or transmit notifications to one or more designated persons. Lamb, [0029], [0040], [0050], [0058]-[0061]. Conversely, if a person is not detected inside the premises, the **barrier alarm device's processor 300** generates an alarm signal and provides it to **transmitter 308** for transmission to **central security panel 116** to initiate an immediate alarm signal. Lamb, [0037], [0041], [0051]-[0053]. In the alternative, the **central security panel 116** may instead receive signals from the **barrier alarm device** regarding the respective statuses of each of the **barrier status detection device 306** and the **human detection device 304**. Lamb, [0043]. Based on these signals, the **central security panel 116** can then determine how and when to respond, and send signals in response accordingly. Lamb, [0043].

2. U.S. 6,057,764 ("Williams") Overview and Motivation to Combine with Lamb

50. **Williams** is directed to a system for providing protection to authorized individuals in a secure space while retaining security against intruders, and is therefore in the same field of endeavor as the '340 patent and **Lamb** – namely, security and alarm systems. '340, 1:15-18; Lamb, [0002]; Williams, 1:6-2:42. Figure 1 below (annotated) illustrates a room where **door alarm switch 13**, **motion detector 14**, and **control panel 17** are installed:

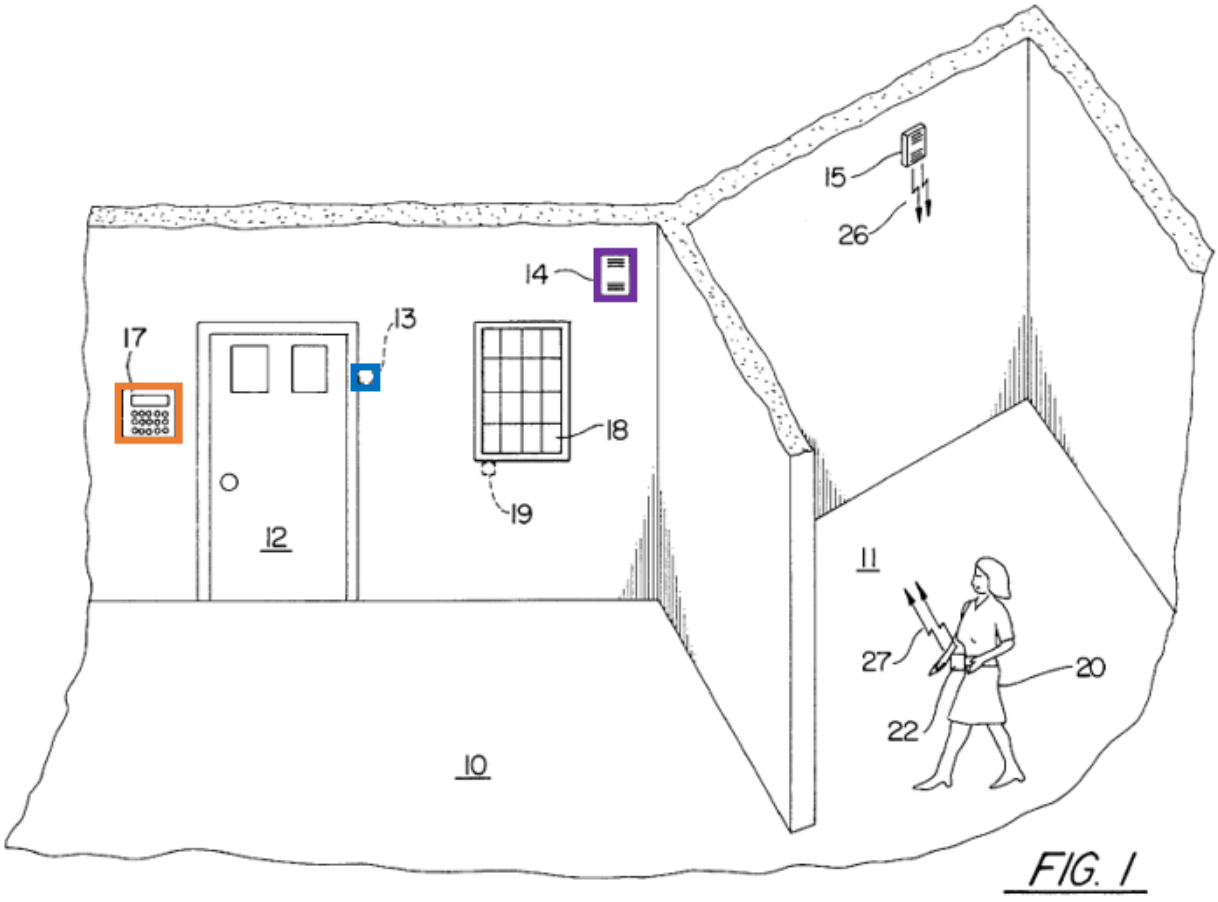


FIG. 1

51. In particular, **Williams** discloses that its system "inquire[s] … whether … there is an authorized user in the space" for "each activation of a motion detector." Williams, 1:64-2:8. If an authorized user properly responds to this inquiry, the "proper response will negate an alarm." Williams, 1:64-2:8. For example, **control panel 17** responds to potential alarms by determining whether an authorized person likely caused the motion based on an activation of **door alarm switch 13** (which detects when a door is opened) or a motion detected by **motion detector 14** (which indicates human movement in the vicinity). Williams, 2:66-3:38, 3:49-4:39.

Specifically, **control panel 17** starts a timer to establish the period of time it will wait to receive an authorization code from an authorized personal device. Williams, 3:49-4:39. If the period of time monitored by the timer expires before such an authorization code is received from such an authorized device, then an alarm is triggered. Williams, 1:64-2:8, 4:32-39. Therefore, **Williams** clearly discloses the use of a timed alarm signal because the signals that **control panel 17** receives from **door alarm switch 13** and **motion detector 14** cause **control panel 17** to set and start a timer, which, if allowed to expire, triggers a security response.

52. As explained in §VII.A.1, **Lamb** discloses that upon a determination by the **barrier alarm device** that a **barrier** has been opened, the system then determines that a person is inside the premises using a **human detection device**, transmits a "bypass signal" to **central security panel 116** to ignore future alarm signals and/or disarm the system because the detected human is considered an "authorized" person. Lamb, [0037], [0040], [0058]-[0059]. It would have been obvious to a person having ordinary skill in the art to enhance system security by modifying **Lamb** to instead transmit a timed alarm signal and wait to receive an authorization code from an authorized device before the timer elapses, as taught by **Williams**.

53. Both **Lamb** and **Williams** describe that their respective systems were designed to help secure a premise without triggering false alarms when authorized

individuals are using the premises, thereby enabling these individuals to have free use of the premises. Lamb, [0005]-[0006]; Williams, 1:13-2:38. And, of course, unauthorized individuals are not desired and may be cause for alarm. Lamb, [0041], [0050]; Williams, 1:13-2:38, 5:63-66. While **Lamb** discloses that its system uses the simple detection of motion within the premises in proximity to the monitored barrier to determine that an authorized person is within the premises (*see* Lamb, [0040] ("this situation indicates that an authorized person inside the premises has opened the barrier"), a person having ordinary skill in the art would have immediately recognized that **Lamb**, in so doing, is simply making an assumption about the person. **Lamb** discloses no way of actually discerning whether the person triggering the motion detector is a person "authorized" to be on the secured premises. **Williams** also discloses a system that permits an alarm to be bypassed upon determination that the detected individual is an authorized person; however, **Williams** further explicitly teaches the known improvement of actually verifying an individual's authorization—and therefore that they are not unauthorized—by using of a timed alarm signal that sets a period of time within which the system expects to receive an authorization code from an authorized device associated with an authorized person. A person having ordinary skill in the art would have therefore been motivated to verify that a potential alarm was triggered by an authorized person, as taught by **Williams**, rather than assume that any detected individual is authorized to enter the

premises like **Lamb's** system. This would have been understood to obviously enhance security by avoiding false alarms but only negating a potential alarm when a detected person is verified as an authorized presence on the premises. As **Williams** explains, such verification can provide an "assurance that unauthorized entry … will be detected," which significantly improves security in **Lamb's** system that assumes authorization based on motion.

54. A person having ordinary skill in the art would have had a reasonable expectation of success when modifying **Lamb's** system to authenticate the individual who is triggering a potential alarm using **Williams's** teaching of a timer and a device configured to transmit an authentication code that can disable an alarm that will otherwise be triggered if the timer elapses. **Lamb** discloses that both its **barrier alarm device** and **central security panel** are capable of monitoring time elapsed and also transmitting, receiving, and processing signals between each other and other devices that are part of a larger system including gateways, servers, and remote devices. Lamb, [0030]-[0037], [0043]. A person having ordinary skill in the art would have found it obvious and straightforward to implement the signal processing steps taught by **Williams** to then use the timing and communication features of Lamb's components to achieve verifiable authentication of an occupant of the secured premises.

3. Invalidity of Claims 1-2, 6, 11-12, and 16 Over Lamb in view of Williams

(a) Element [1.pre]

55. **Element [1.pre] recites "A barrier alarm device, comprising."** This element is met by Lamb.

56. **Lamb discloses a barrier alarm device** (*e.g.*, a "barrier alarm device"). *See*, *e.g.*, Lamb (emphasis added):

- **Fig. 3:**

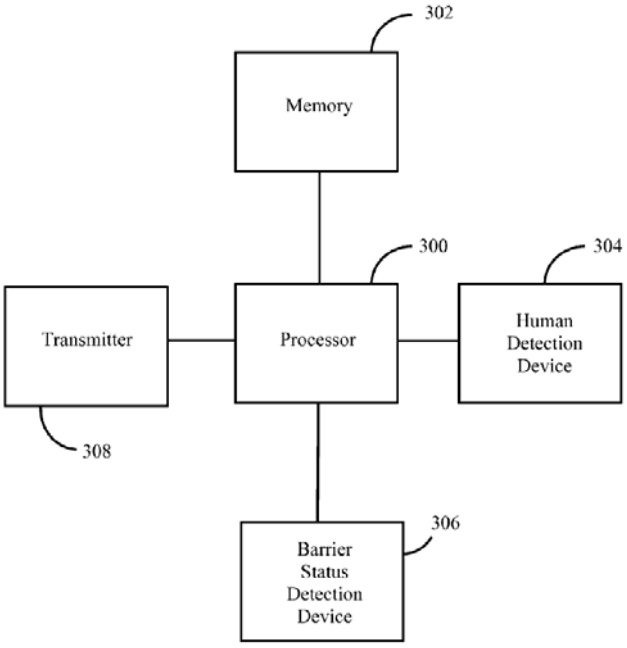


FIG. 3

- **Fig. 4:**

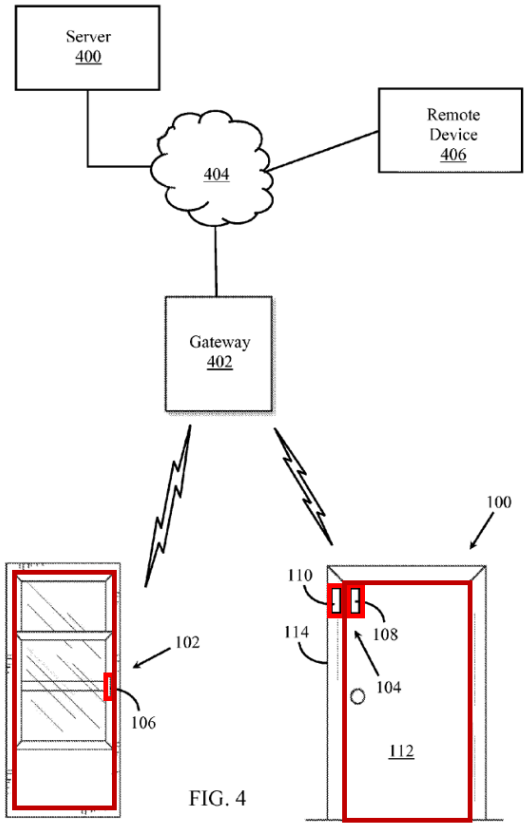


FIG. 4

- **[0017]** ("The present application relates to *barrier alarm devices, such as door or window sensors*, that have a capability of reducing occurrences of false alarms. For the purpose of the discussions herein, *the term "barrier alarm device" means any device used to monitor and report states, physical conditions, attributes, status, or parameters of an entrance/exit barrier such as a door, a window, a gate, etc.* Examples of barrier alarm devices comprise door and window sensors, glass breakage detectors, light interruption detectors, etc.")
- **[0019]** ("FIG. 1 is an illustration of a security system in accordance with one embodiment of the principles discussed herein. *In this embodiment a door assembly 100 and a window assembly 102 are monitored by barrier alarm devices 104 and 106, respectively.* In one embodiment, barrier alarm device 104 comprises magnet 108 mounted to door 112 and reed switch assembly 110 mounted to door frame 114, while barrier alarm device 106 comprises a magnet-less type sensor. The barrier alarm devices could, use alternative techniques to magnetic field sensing to determine that status of a door or a window.")
- **[0030]** ("*FIG. 3 is a functional block diagram of one embodiment of a portion of barrier alarm device 104 or 106* in accordance with the teachings

herein. Specifically, FIG. 3 shows processor 300, memory 302, human detection device 304, a barrier status detection device 306, and transmitter 308.")

- **[0039]** ("FIG. 4 is an illustration of another security system in accordance with another embodiment of the principles discussed herein. In this embodiment, *barrier alarm devices 104 and 106* communicate with a receiver such as gateway 402, which forwards communications from the barrier alarm devices to remote server 400 via wide area network 404. In one embodiment, the barrier alarm devices additionally may communicate with a second receiver, such as central alarm panel 116, as discussed previously.")
- ***See also* Fig. 1.**

57. **Lamb** clearly discloses a **barrier alarm device**: both "**barrier alarm device 104**" that monitors "**door assembly 100**" and "**barrier alarm device 106**" that monitors "**window assembly 102**" are examples of barrier alarm devices.

(b) Element [1.a]

58. **Element [1.a] recites "a barrier status detection device for indicating that a barrier monitored by the barrier alarm device has been opened."** This element is met by Lamb.

59. **Lamb discloses a barrier status detection device for indicating that a barrier monitored by the barrier alarm device has been opened** (*e.g.*, "barrier status detection device" for providing signals "indicative of changes in … physical conditions …, such as the condition of a door or window being 'open' or 'closed'"**).** *See, e.g.*, Lamb (emphasis added):

- **Fig. 3:**

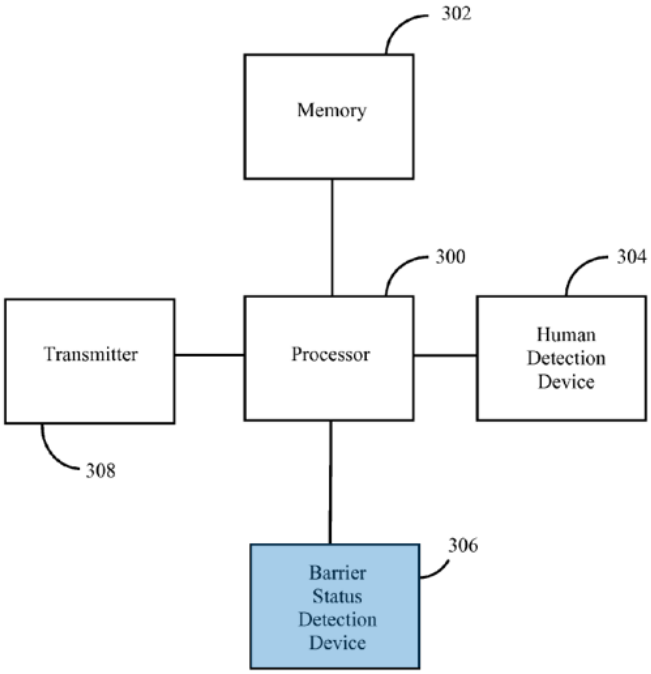


FIG. 3

- **[0030]** ("*FIG. 3 is a functional block diagram of one embodiment of a portion of barrier alarm device 104 or 106* in accordance with the teachings herein. Specifically, FIG. 3 shows processor 300, memory 302, human detection device 304, a barrier status detection device 306, and transmitter 308.")
- **[0033]** ("*Barrier status detection device 306* is coupled to processor 300 and *monitors or determines a state, physical condition, attribute, status, or parameter of something, such as the status (e.g., "open", "closed", "movement detected", etc.) of a door, window, gate, or other entrance or exit barrier*. Barrier status detection device 306 may comprise a reed switch, ultrasonic transducer/receiver, an infrared transmitter/receiver, an RFID receiver, a tilt sensor, an accelerometer, a gyroscope, a motion sensor, or some other device *to determine whether a window is open or closed*.")
- ***See also* [0037].**

60. **Lamb** clearly discloses that its **barrier alarm device** includes a **barrier detection device 306** that monitors and detects whether a door or window has been opened. Lamb, [0030], [0033]. The barrier detection device may be

implemented as "ultrasonic transducer/receiver, an infrared transmitter/receiver, an RFID receiver, a tilt sensor, an accelerometer, a gyroscope, a motion sensor, or some other device." Lamb, [0033].

(c) Element [1.b]

61. **Element [1.b] recites "a human detection device for indicating that a human being is inside a premises in proximity to the barrier."** This element is met by Lamb.

62. **Lamb discloses a human detection device for indicating that a human being is inside a premises in proximity to the barrier** (*e.g.*, "human detection device" for "detecting[ing] the presence of a person in proximity to the barrier alarm device, either inside a monitored premises, outside a monitored premises, or both")**.** *See, e.g.*, Lamb (emphasis added):

- **Fig. 3:**

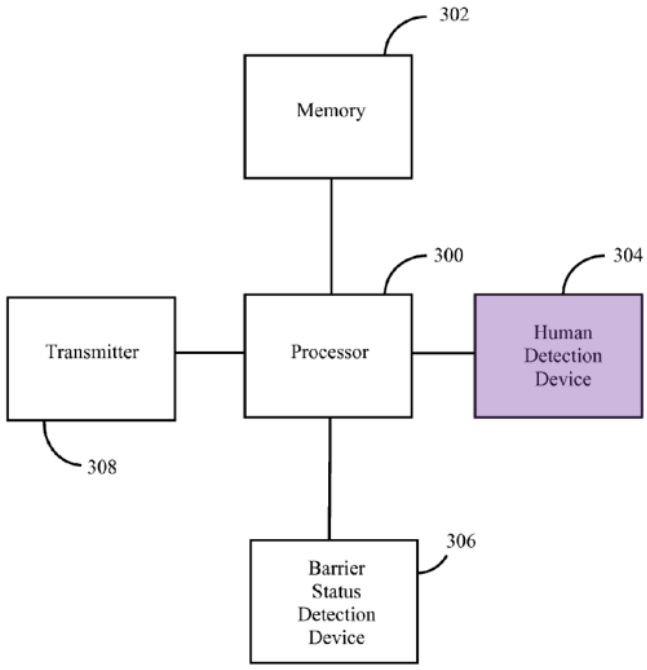


FIG. 3

- **[0034]** ("*Human detection device 304* comprises a device or circuitry *to detect the presence of a person in proximity to the barrier alarm device*, either *inside a monitored premises*, outside a monitored premises, or both. Examples of human detection device 304 include an ultrasonic transducer/receiver, an infrared transmitter/receiver, a capacitance sensor, an RF tank circuit, an RFID receiver and RFID chip, a motion detector, or some other circuitry or device able to detect the presence of a human being proximate to the barrier alarm device, door, or window. The term "proximate to the barrier alarm device, door or window" means that a person is within a distance from a barrier alarm device, door, or window that the person could open the door or window where a barrier alarm device is installed.")
- ***See also* [0035].**

63. **Lamb** discloses that its **barrier alarm device** includes a **human detection device 304** that monitors for and detects the presence of a person proximate to the barrier alarm device, door, or window. Lamb, [0034]. The **human**

detection device 304 may be implemented as "an ultrasonic transducer/receiver, an infrared transmitter/receiver, a capacitance sensor, an RF tank circuit, an RFID receiver and RFID chip, a motion detector, or some other circuitry or device." Lamb, [0034].

(d) Element [1.c]

64. **Element [1.c] recites "a transmitter for transmitting a timed alarm signal to a receiver associated with a security panel, the timed alarm signal for initiating a timer associated with the security panel."** This element is met by Lamb in view of Williams.

65. **Lamb discloses a transmitter** (*e.g.*, "transmitter") **for transmitting an alarm signal to a receiver associated with a security panel** (*e.g.*, for transmitting an alarm signal "to a remote location, such as central security panel 116 or a gateway")**.** *See*, *e.g.*, Lamb (emphasis added):

- **Fig. 1:**

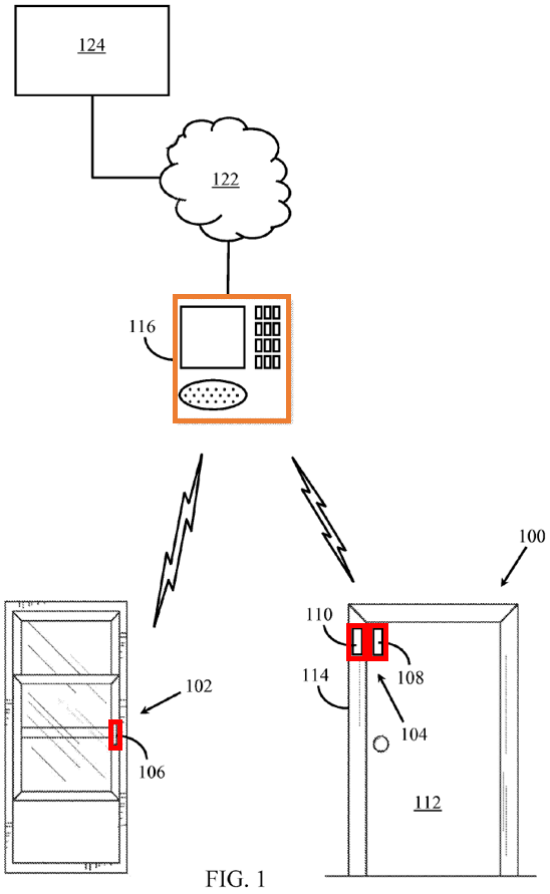


FIG. 1

- **Fig. 3:**

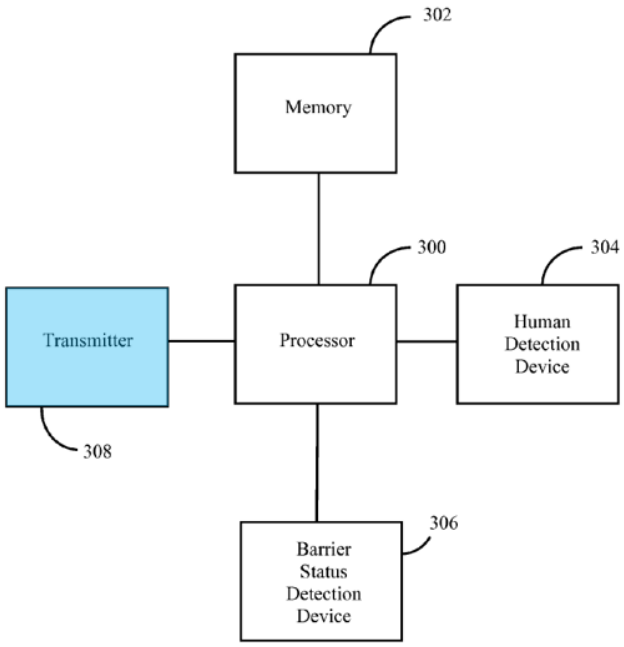


FIG. 3

- **[0020]** ("*Each of the barrier alarm devices communicates with receiver, such as central security panel 116, typically using wireless RF signals generated by the barrier alarm devices and/or central security panel 116*. For example, if door 112 is opened, reed switch assembly 110 detects a reduction or elimination of a magnetic field produced by magnet 108 as magnet 108 moves away from reed switch assembly 110 as door 112 is opened. In response, reed switch assembly 110 transmits a message to central security panel 116 indicative of a local alarm condition, e.g., door 112 has been opened.")
- **[0036]** ("*Transmitter 308 comprises circuitry necessary to wirelessly transmit alarm signals and/or status messages and/or other information from the barrier alarm device to one or more receivers, such as central security panel 116 or a gateway device* coupled to a wide area network such as the Internet, either directly or through in intermediate device, such as a repeater, commonly used in popular mesh networks. Such circuitry is well known in the art and may comprise BlueTooth, Wi-Fi, RF, optical, ultrasonic circuitry, among others. Alternatively, or in addition, transmitter 308 comprises well-known circuitry to provide signals to central security panel 116 or a gateway via wiring, such as telephone wiring, twisted pair, two-conductor pair, CAT wiring, AC home wiring, or other type of wiring.")

- **[0037]** ("In any case, if processor 300 determines that a local alarm condition has occurred, *an alarm signal is provided to transmitter 308 for transmission to a remote location, such as central security panel 116 or a gateway*. In one embodiment, the alarm signal comprises a notification to central security panel 116 that a local alarm condition has been detected at a particular door or window being monitored by the barrier alarm device.")
- **[0041]** ("The alarm signal may also be *transmitted from the barrier alarm device to central security panel 116*.")
- ***See also*** **[0022], [0029].**

66. **Williams discloses a transmitter for transmitting a timed alarm signal to a receiver associated with a security panel** (*e.g.*, a motion detector providing, via electromagnetic radiation to a control panel, a "violation signal indicative of a potential alarm in response to sensing motion within a space")**, the timed alarm signal for initiating a timer associated with the security panel** (*e.g.*, in response to receiving a signal when a human is detected, "control panel" initializes a timer that, upon timing out without receiving an authorized code, sets an alarm)**.** *See, e.g.*, Williams (emphasis added):

- **Fig. 2:**

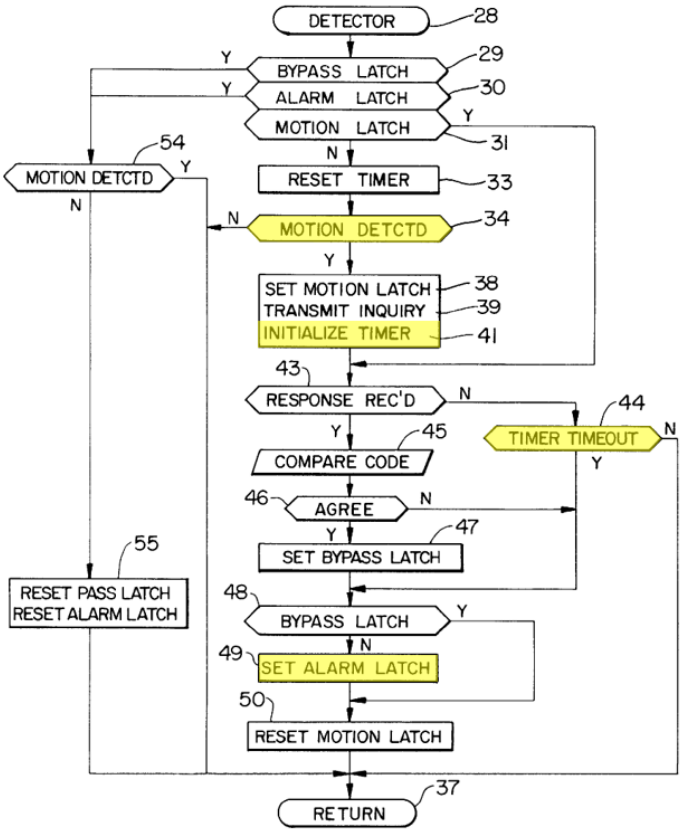


FIG. 2

- **Fig. 2A:**

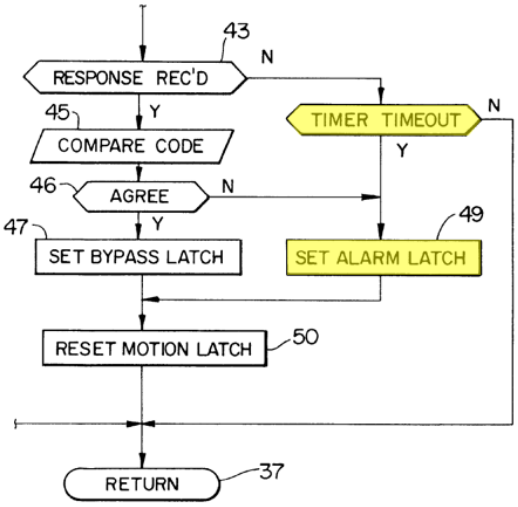


FIG. 2A

- **1:64-2:8** ("*[E]ach activation of a motion detector causes a corresponding transceiver to inquire*, by an electromagnetic transmission, *whether or not there is an authorized user in the space*, the portable device of the authorized user responding to the electromagnetic transmission with an appropriate code, *whereby a proper response will negate an alarm*.")
- **3:9-38** ("In operation, *should the motion detector for instance, sense motion of the person 20, an interrogation* by electromagnetic radiation … *will be received by the portable device 22, which in turn will respond with electromagnetic radiation … in like kind with the transmission of the motion detector 15, the transmission from the device 22 including a code to authenticate the authority of the user to be within the secure space while the alarm is on*…. Every possible switch or other sensor which could enter an alarm condition may similarly be provided with a transceiver, if desired…. For instance, *a transceiver within the control panel [17] may do the inquiry* for a potential alarm created by the switch 13 on the entry door 12 as well as *for a potential alarm created by motion within the room 10*. Suffice it to say that any potential alarm condition can be associated with a challenge for an authorization signal to cause the potential alarm condition to be deemed to not be a breach of the secure space.")
- **3:49-4:39** ("Referring now to FIG. 2, *a detector routine which performs the function of the invention with respect to a corresponding sensor, is reached through an entry point 28* and a first set of tests 29-31 determines if a pass latch, an alarm latch or a motion latch (described hereinafter) has been set or not. Prior to sensing motion, all three latches will not have been set, so negative results of tests 29-31 will reach a step 33 to reset a timer, as described more fully hereinafter. Then *a test 34 determines if the corresponding motion detector has detected motion. … [I]f motion has been detected, an affirmative result of test 34 will reach a step 38 to set the motion latch*, so that future passes through the routine of FIG. 2 will not go through the step 33 or the test 34, as described hereinafter. Then, *a step 39 causes an inquiry signal to be transmitted to determine if there is an authorized personal device within the proximity of the detector to which this routine relates. And, a step 41 initializes a timer to establish a period of time (perhaps a second or fraction thereof) within which an authorized response must be received.* [¶] *A test 43 determines if a response has been received, and if not, a negative result reaches a test 44 to determine if the timer, initialized in step 41, has timed out or not.* Initially, it may not, so a negative result of test 44 reaches the return point 37 to free-up the computer for other tasks. In the next pass through the routine of FIG. 2, tests 29 and 30 are still

negative but test 31 is affirmative, returning the routine to test 43 to determine if a response has been received or not. *If a response has been received, an affirmative result of test 43 reaches a subroutine 45 to compare the authorization code within the response to the predetermined authorization code…. Then a test 46 determines if the two codes agree. If they do agree, an affirmative result of test 46 reaches a step 47 to set a bypass latch to indicate that this incidence of motion detection has responded to inquiry and has been authenticated.* Following comparison of the codes in the subroutine 45, if the test 46 is negative because the proper code was not received, the step 47 is bypassed. Then a test 48 determines if the bypass latch has been set or not; if not, an alarm latch is set in a step 49; but if the bypass latch is set, an affirmative result of test 48 avoids setting the alarm latch…. *On the other hand, if no response is received prior to time-out of the timer, the test 44 will be affirmative reaching the test 48 and the step 49 to similarly set the alarm latch. In other words, if a wrong code is received or no code is received, the alarm latch will be set in the step 49.* Thereafter, the step 50 will reset the motion latch to enable a future cycle of operation, and other programming is reverted to through the return point 37.")

- **7:43-63** ("*In any system which utilizes a warning sound and a delay in entering an alarm, as is typical at entry doors of conventional systems, then the present invention may be practiced by allowing the arming condition to go into effect, during which time if there is an authorized user, it will deactivate the alert condition causing the warning sound to cease and cancelling the alarm.*")
- **Claim 1** ("An alarm system comprising: one or more *motion detectors for providing a violation signal indicative of a potential alarm in response to sensing motion within a space…*")
- ***See also* Abstract, 2:11-18, Claims 5 and 8.**

67. **Lamb** discloses that its **barrier alarm device** includes a **transmitter 308** component that can be used to transmit alarm signals to a **central security panel 116**.

68. A person having ordinary skill in the art would have recognized that despite **Lamb's** failure to *expressly* disclose that **central security panel 116**

includes an associated "receiver" for receiving alarm signals from the **barrier alarm device**, **central security panel 116** must necessarily include a receiver based on **Lamb's** disclosures that the **barrier alarm device** and **central security panel 116** communicate via such mechanisms including Wi-Fi, RF, and telephone wiring. These transmitted electromagnetic signals, which travel through the air and/or wires to the **central security panel 116**, must be "received" by a "receiver" associated with the **central security panel 116**.

69. Even if **Lamb** does not explicitly disclose transmitting a "timed alarm signal for initiating a timer associated with the security panel," a person having ordinary skill in the art would have been motivated to modify **Lamb's** teachings to include transmission of a timed alarm signal that initiates a timer when the **barrier alarm device** detects that the barrier has been opened and that a human is inside the premises, as taught by **Williams**. A person having ordinary skill in the art would have understood this modification to provide significantly greater protection to individuals in the premises since it enables verification that the potential alarm is indeed caused by an authorized person by providing time for such verification, as discussed in §VII.A.2.

70. **Williams** discloses that after "a potential alarm [is] created by motion within the room," a "transceiver within the control panel" is directed to "inquir[e]" whether an "authorized user" with an "appropriate code" is in the monitored space,

"whereby a proper response will negate an alarm." Williams, 1:64-2:8, 3:19-38. In this way, **Williams** provides a way verify the identity of the detected individual, which a person having ordinary skill in the art would have understood to achieve better security for the monitored premises.

71. For example, as shown in Figure 2, **Williams** discloses that after a determination that motion has been detected (test 34), its system responds with an inquiry for an authorized code (step 39) and initializes a timer "to establish a period of time … within which an authorized response must be received" (step 41). Williams, 3:56-4:3. If no response is received from an authorized user (test 43) before the timer elapses (test 44), then an alarm latch is set to trigger an alarm notification (step 49). Williams, 4:4-36. If an authorized response is received (test 43) before the timer elapses, then a bypass latch is set (step 47) that causes the alarm (step 49) to be bypassed (test 48). Williams, 4:12-27. As elaborated in Fig. 2A, the alarm latch may be set directly after the timeout of the timer. Williams, 5:3-5. Accordingly, **Williams** discloses that its "control panel" initializes a timer in response to receiving a signal that a human has been detected— therefore, a person having ordinary skill in the art would have understood **Williams'** signal to be a timed

alarm signal associated with the control panel.[3] When the timer elapses, if no response is received from an authorized user, the control panel sets an alarm to indicate an intrusion.

(e) Element [1.d]

72. **Element [1.d] recites "a memory having processor-executable instructions stored thereon."** This element is met by Lamb.

73. **Lamb discloses a memory** (*e.g.*, "memory") **having processor-executable instructions stored thereon.** *See*, *e.g.*, Lamb (emphasis added):

[3] I understand the claimed "timed alarm signal" to refer only to the step of "for initiating a timer" associated with the security panel. I understand that "alert(s)" and "security response(s)" are separate elements in other claims of the '340 patent. *See*, *e.g.*, claims [6.h]-[6.i], 13, [16.e].

- **Fig. 3:**

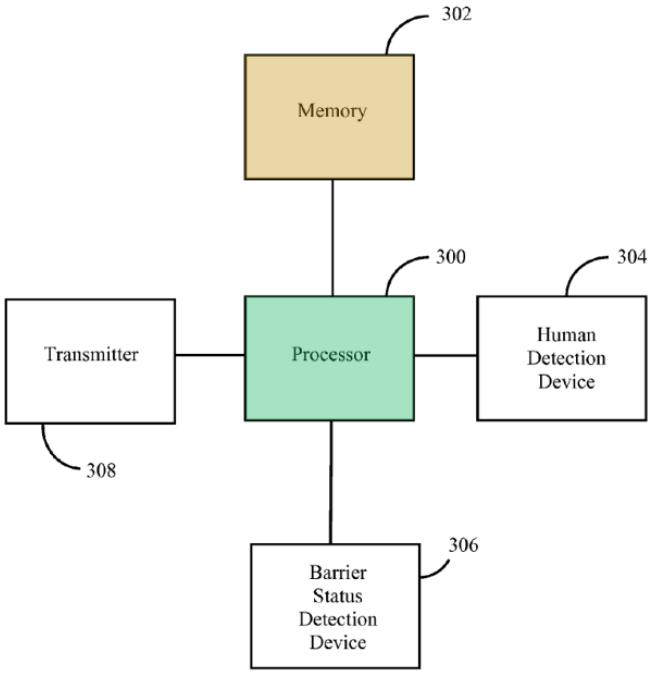


FIG. 3

- **[0032]** ("Memory 302 comprises one or more information storage devices, such as RAM memory…. *Memory 302 is used to store processor-executable instructions for operation of the barrier alarm device as well as any information used by processor 300*, such as threshold information, parameter information, identification information, current or previous door or window status information, etc.")

74. **Lamb** discloses that its **barrier alarm device** includes "**memory 302**" that stores "processor-executable instructions for operation of the barrier alarm device." Lamb, [0032].

(f) Element [1.e]

75. **Element [1.e] recites "a processor coupled to the barrier status detection device, the human detection device, the transmitter, and the memory,**

for executing the processor-executable instructions that cause the barrier alarm device to." This element is met by Lamb.

76. **Lamb discloses discloses a processor** (*e.g.*, "processor") **coupled to the barrier status detection device, the human detection device, the transmitter, and the memory, for executing the processor-executable instructions.** *See*, *e.g.*, Lamb (emphasis added):

- **Fig. 3:**

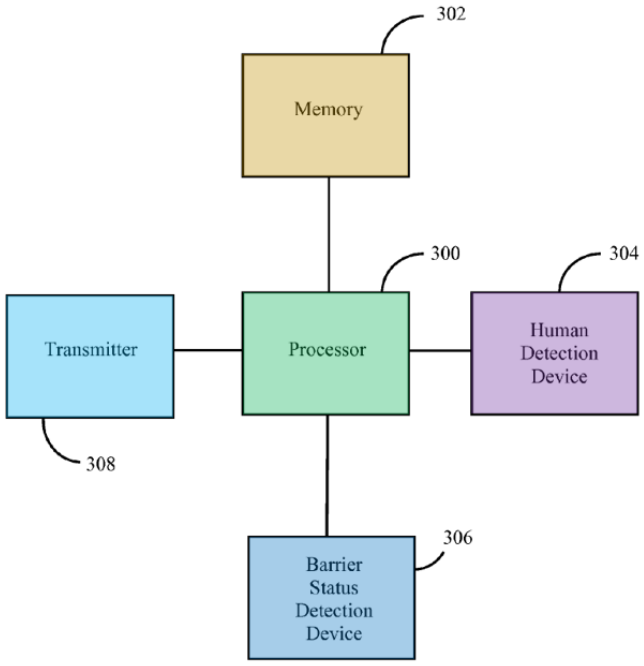


FIG. 3

- **[0030]** ("*FIG. 3 is a functional block diagram of one embodiment of a portion of barrier alarm device 104 or 106* in accordance with the teachings herein. Specifically, FIG. 3 shows processor 300, memory 302, human detection device 304, a barrier status detection device 306, and transmitter 308.")
- **[0031]** ("Processor 300 is configured to provide general operation of the barrier alarm device by executing processor-executable instructions stored in memory 302, for example, executable code. Processor 300 typically

comprises a general purpose processor…, although any one of a variety of microprocessors, microcomputers, and/or microcontrollers may be used alternatively.")

- **[0032]** ("Memory 302 comprises one or more information storage devices, such as RAM memory…. *Memory 302 is used to store processor-executable instructions for operation of the barrier alarm device as well as any information used by processor 300*, such as threshold information, parameter information, identification information, current or previous door or window status information, etc.")
- **[0033]** ("*Barrier status detection device 306* is coupled to processor 300 and *monitors or determines a state, physical condition, attribute, status, or parameter of something, such as the status (e.g., "open", "closed", "movement detected", etc.) of a door, window, gate, or other entrance or exit barrier.* Barrier status detection device 306 may comprise a reed switch, ultrasonic transducer/receiver, an infrared transmitter/receiver, an RFID receiver, a tilt sensor, an accelerometer, a gyroscope, a motion sensor, or some other device *to determine whether a window is open or closed*.")
- **[0035]** ("[W]hen a person approaches a door or window monitored by the barrier alarm device…, *human detection device 304 sends a signal to processor 300* when the person is within a predetermined distance from the barrier alarm device and, thus, the monitored door or window. In another embodiment, human detection device 304 is inactive until barrier status detection device 306 determines that a monitored door or window has been opened. In this embodiment, *barrier status detection device 306 sends a signal to processor 300, and processor 300 then activates the human detection device 304* to determine if a person is proximate to the barrier alarm device and, thus, the monitored door or window, either inside the monitored premises, outside, or both.")
- ***See also* [0037], [0043]-[0061].**

77. **Lamb** discloses that its **barrier alarm device** includes a **processor 300** that can communicate via signals with the **barrier status detection device 306**, the **human detection device 304**, the **transmitter 308**, and the **memory 302**. The **processor 300** directs the execution of the processor-executable instructions that are stored in the **memory 302** to control operations of the **barrier alarm device**.

(g) Element [1.f]

78. **Element [1.f] recites "respond to the barrier status detection device indicating that the barrier has been opened by determining whether the human detection device indicates that the human being is inside the premises in proximity to the barrier."** This claim is met by Lamb.

79. **Lamb discloses the processor executing the processor-executable instructions to cause the barrier alarm device to** (*e.g.*, *see* [1.e]) **respond to the barrier status detection device indicating that the barrier has been opened by determining whether the human detection device indicates that the human being is inside the premises in proximity to the barrier** (*e.g.*, "[i]f processor 300 determines that a door or window has been opened, it checks to see whether human detection device 304 has sensed a person proximate to the barrier alarm device, door, or window," such as being "inside a monitored premises")**.** *See*, *e.g.*, Lamb (emphasis added):

- **Fig. 5:**

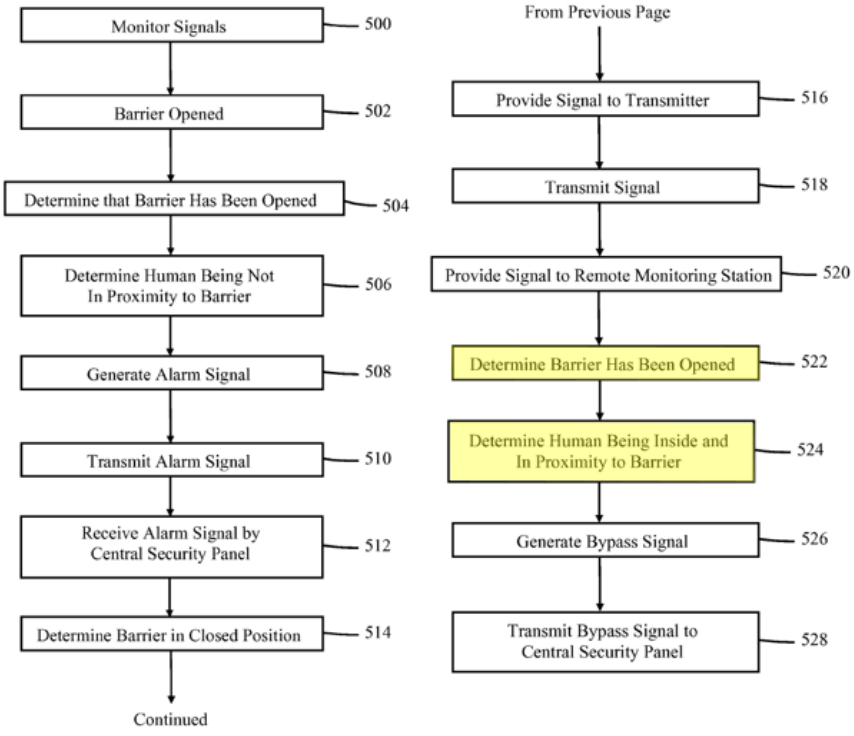


FIG. 5

FIG. 5
Continued

- **[0037]** ("In normal operation, processor 300 executes processor-executable instructions stored in memory 302 that causes *processor 300 to monitor signals provided by barrier status detection device 306 indicative of changes in one or more states*, physical conditions, attributes, status, or parameters of something being monitored, *such as the condition of a door or window being "open" or "closed"*, changes between these states, or simply "movement". *Processor 300 uses this data from barrier status detection device 306 to determine whether a predetermined condition has occurred relating to the barrier alarm device (herein "local alarm condition"), such as a door or window being monitored by the barrier alarm device changing state from "closed" to "open", movement between these states, or simply "movement".* Human detection device 304 monitors for the presence of a person proximate to the barrier alarm device, door or window and provides signals to processor 300 indicative of whether a human being is proximate or not. *If processor 300 determines that a door or window has been opened, it checks to see whether human detection device 304 has sensed a person proximate to the barrier alarm device, door, or window.…*. In any case, if processor 300 determines that a local alarm condition has occurred, an alarm signal is provided to transmitter 308 for transmission to a remote location,

such as central security panel 116 or a gateway. In one embodiment, the alarm signal comprises a notification to central security panel 116 that a local alarm condition has been detected at a particular door or window being monitored by the barrier alarm device.")

- **[0040]** ("In one embodiment, *when a barrier alarm device detects that a barrier, such as a door or a window, has been opened, and further that a human being is inside the premises being monitored in proximity to the barrier* … this situation indicates that an authorized person inside the monitored premises has opened the barrier.")
- **[0058]-[0059]** ("At block 522, after the barrier has been closed, *processor 300 determines that the barrier has been opened by detecting a change in a signal from barrier status detection device 306*. [¶] At block 524, *processor 300 determines that a human being is inside the premises in proximity to the barrier by evaluating the signals from human detection device 304*.")

80. *See* my discussion of elements [1.a]-[1.b] and [1.d]-[1.e]. In addition, **Lamb** discloses that **processor 300** in the **barrier alarm device** processes data from two different detection devices: the **barrier status detection device 306** (which sends signals indicating whether a door is open) and the **human detection device 304** (which sends signals indicating a human is proximate to a door inside a premises). Lamb, [0037]. In one such process, Lamb teaches that "if" the **barrier status detection device 306** indicates that a door is "open," the **processor 300** then proceeds to determine whether **human detection device 304** indicates that a human is inside a premises. Lamb, [0037], [0040]. *See*, *e.g.*, steps 522 and 524. Lamb, Fig. 5, [0058]-[0059].

(h) Element [1.g]

81. **Element [1.g] recites "transmit, via the transmitter, the timed alarm signal to the receiver only when it is determined that the human detection**

device indicates that the human being is inside the premises in proximity to the barrier." This claim is met by Lamb in view of Williams.

82. **Lamb discloses the processor executing the processor-executable instructions to cause the barrier alarm device to** (*e.g.*, *see* [1.e]) **transmit, via the transmitter, a signal to the receiver** (*e.g.*, transmit to the receiver associated with central security panel 116 (*see* [1.c]), a bypass signal) **only when it is determined that the human detection device indicates that the human being is inside the premises in proximity to the barrier** (*e.g.*, "when [the] barrier alarm device detects … that a human being is inside the premises being monitored in proximity to the barrier")**.** *See*, *e.g.*, Lamb (emphasis added):

- **Fig. 5:**

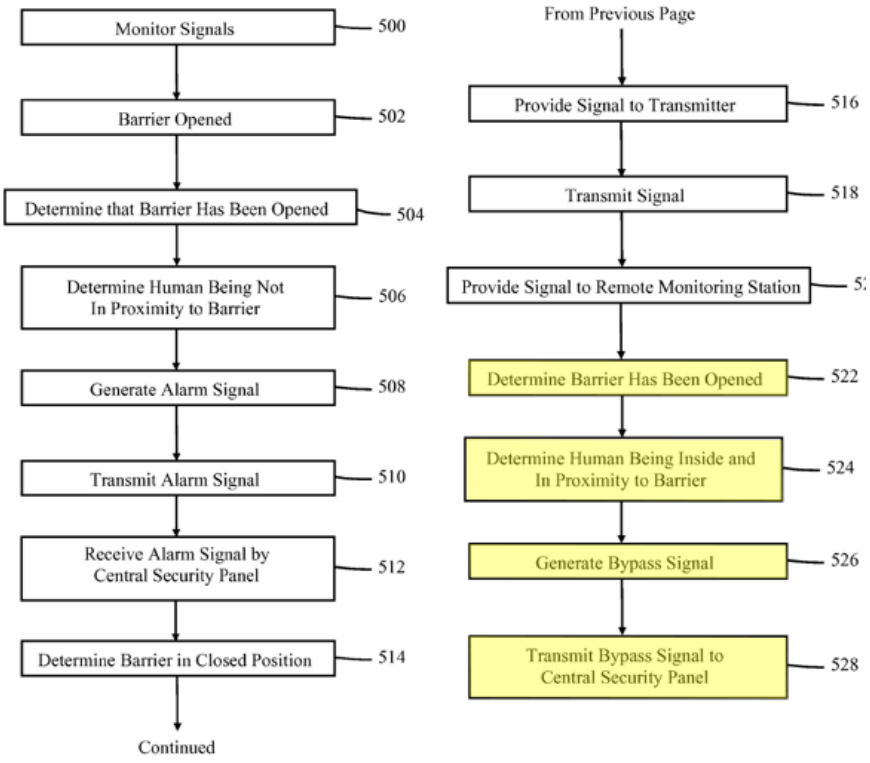


FIG. 5

FIG. 5
Continued

- **[0040]** ("In one embodiment, *when a barrier alarm device detects* that a barrier, such as a door or a window, has been opened, and further *that a human being is inside the premises being monitored in proximity to the barrier*, the barrier alarm device does not send an alarm signal to gateway 402, as *this situation indicates that an authorized person inside the monitored premises has opened the barrier*. In another embodiment, *a bypass signal is transmitted to central security panel 116*, as described above.")
- **[0060]** ("*At block 526, in response to determining that the barrier has been opened and that a human being is inside the premises in proximity to the barrier detection device*, processor 300 may refrain from sending an alarm signal to central security panel 116 and gateway 402. *Additionally, or alternatively, processor 300 generates a bypass signal and provides the bypass signal to transmitter 308 where it is transmitted to central security device 116 and/or gateway 402.* The bypass signal is an instruction to central security panel 116 to ignore future alarm signals generated by the barrier alarm device. The bypass signal may, additionally or alternatively, cause central security panel 116 to disarm the entire security system and to notify one or more persons that the security system has been disarmed, and/or that

> a barrier has been opened by an authorized person. Similarly, the bypass signal, or a different signal, may be transmitted to gateway 402 to provide an indication to remote server 400 that a barrier has been opened by an authorized person and to ignore future alarm signals generated by the barrier alarm device until the barrier is again placed into the closed position.")

- ***See also*** **[0037], [0050], [0058]-[0059].**

83. **Williams discloses transmitting the timed alarm signal to the receiver** (*see* [1.g]) **when it is determined that the human detection device indicates that the human being is inside the premises in proximity to the barrier** (*e.g.*, in response to receiving a signal when a human is detected, "control panel" initializes a timer that, upon timing out without receiving an authorized code, sets an alarm)**.** *See*, *e.g.*, Williams (emphasis added):

- **Fig. 2**

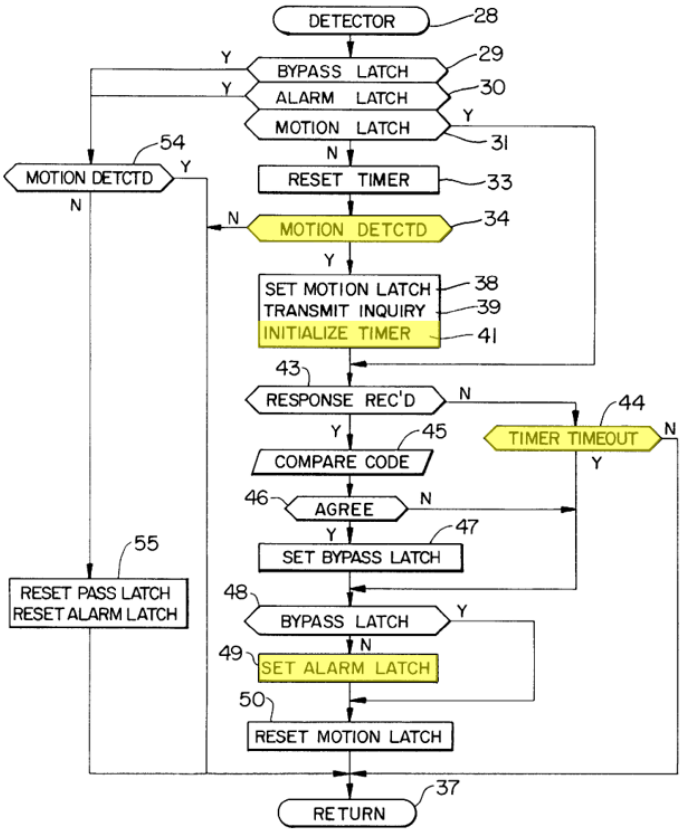


FIG. 2

- **Fig. 2A**

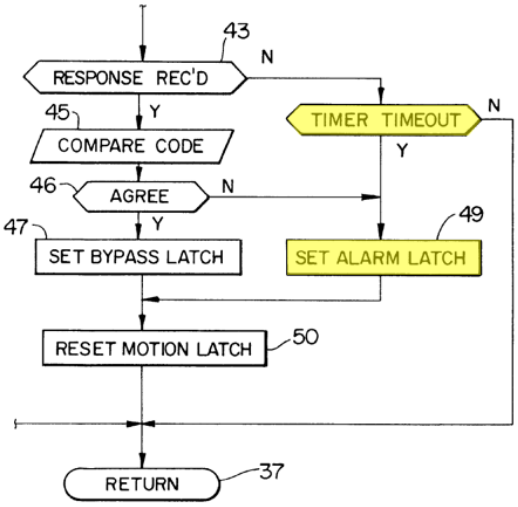


FIG. 2A

- **1:64-2:8** ("*[E]ach activation of a motion detector causes a corresponding transceiver to inquire*, by an electromagnetic transmission, *whether or not there is an authorized user in the space*, the portable device of the authorized user responding to the electromagnetic transmission with an appropriate code, *whereby a proper response will negate an alarm*.")
- **3:9-38** ("In operation, *should the motion detector for instance, sense motion of the person 20, an interrogation* by electromagnetic radiation … *will be received by the portable device 22, which in turn will respond with electromagnetic radiation … in like kind with the transmission of the motion detector 15, the transmission from the device 22 including a code to authenticate the authority of the user to be within the secure space while the alarm is on*…. Every possible switch or other sensor which could enter an alarm condition may similarly be provided with a transceiver, if desired…. For instance, *a transceiver within the control panel [17] may do the inquiry* for a potential alarm created by the switch 13 on the entry door 12 as well as *for a potential alarm created by motion within the room 10*. Suffice it to say that any potential alarm condition can be associated with a challenge for an authorization signal to cause the potential alarm condition to be deemed to not be a breach of the secure space.")
- **3:49-4:39** ("Referring now to FIG. 2, *a detector routine which performs the function of the invention with respect to a corresponding sensor, is reached through an entry point 28* and a first set of tests 29-31 determines if a pass latch, an alarm latch or a motion latch (described hereinafter) has been set or not. Prior to sensing motion, all three latches will not have been set, so negative results of tests 29-31 will reach a step 33 to reset a timer, as described more fully hereinafter. Then *a test 34 determines if the corresponding motion detector has detected motion*. … *[I]f motion has been detected, an affirmative result of test 34 will reach a step 38 to set the motion latch*, so that future passes through the routine of FIG. 2 will not go through the step 33 or the test 34, as described hereinafter. Then, *a step 39 causes an inquiry signal to be transmitted to determine if there is an authorized personal device within the proximity of the detector to which this routine relates*. And, *a step 41 initializes a timer to establish a period of time (perhaps a second or fraction thereof) within which an authorized response must be received*. [¶] *A test 43 determines if a response has been received, and if not, a negative result reaches a test 44 to determine if the timer, initialized in step 41, has timed out or not.* Initially, it may not, so a negative result of test 44 reaches the return point 37 to free-up the computer for other tasks. In the next pass through the routine of FIG. 2, tests 29 and 30

are still negative but test 31 is affirmative, returning the routine to test 43 to determine if a response has been received or not. *If a response has been received, an affirmative result of test 43 reaches a subroutine 45 to compare the authorization code within the response to the predetermined authorization code*…. *Then a test 46 determines if the two codes agree. If they do agree, an affirmative result of test 46 reaches a step 47 to set a bypass latch to indicate that this incidence of motion detection has responded to inquiry and has been authenticated.* Following comparison of the codes in the subroutine 45, if the test 46 is negative because the proper code was not received, the step 47 is bypassed. Then a test 48 determines if the bypass latch has been set or not; if not, an alarm latch is set in a step 49; but if the bypass latch is set, an affirmative result of test 48 avoids setting the alarm latch…. *On the other hand, if no response is received prior to time-out of the timer, the test 44 will be affirmative reaching the test 48 and the step 49 to similarly set the alarm latch. In other words, if a wrong code is received or no code is received, the alarm latch will be set in the step 49.* Thereafter, the step 50 will reset the motion latch to enable a future cycle of operation, and other programming is reverted to through the return point 37.")

- **7:43-63** ("*In any system which utilizes a warning sound and a delay in entering an alarm, as is typical at entry doors of conventional systems, then the present invention may be practiced by allowing the arming condition to go into effect, during which time if there is an authorized user, it will deactivate the alert condition causing the warning sound to cease and cancelling the alarm.*")
- **Claim 1** ("An alarm system comprising: one or more *motion detectors for providing a violation signal indicative of a potential alarm in response to sensing motion within a space*…")
- ***See also* Abstract, 2:11-18, Claims 5 and 8.**

84. *See* my discussion for elements [1.c]-[1.f]. As discussed for [1.f], **Lamb** discloses that **processor 300** may, depending the circumstances, determine that a monitored door is open and that a human is present inside the premises proximate to the door. Lamb, [0037], [0040], [0058]-[0059]. **Lamb** discloses that that **processor 300** interprets these simultaneous detections of an open door and a human presence

within the premises as indicative "that an authorized person inside the monitored premises has opened the barrier." Lamb, [0040]. Therefore, upon detecting an open door and human presence in the premises, Lamb's **barrier alarm device** transmits a "bypass signal" to **central security panel 116** which can direct the **central security panel 116** to take such actions as ignoring future alarm signals, disarming the system, and/or transmitting notifications regarding the open barrier and/or the status of the system to other parts of the system. Lamb, [0029], [0040], [0050], [0058]-[0061].

85. As discussed in §VII.A.2. and [1.c] above, a person having ordinary skill in the art would have been motivated to modify **Lamb** to also include **Williams's** teaching of transmitting a timed alarm signal when the **barrier alarm device** detects that the monitored barrier has been opened and that a human is present within the relevant premises, providing time to verify the identity of the detected individual via an authorized user before triggering an alarm notification. A person having ordinary skill in the art would have understood this modification to have the predictable benefit of providing significantly greater protection to individuals in the premises by verifying that the detected human is indeed an authorized person, rather than simply assuming any detected individual is authorized, as discussed in §VII.A.2.

86. As discussed for [1.c], **Williams** discloses that potential alarms are created when motions of the barrier and humans are detected, and an appropriate code must be received within a certain time period (monitored by an initialized timer) to stop the setting of an alarm once the time period has elapsed. The signal causing the control panel to initiate this timed process would have been understood by a person having ordinary skill in the art to be a timed alarm signal. *See* [1.c].

(i) Claim [2]

87. **Claim [2] recites "The barrier alarm of claim 1, wherein the processor-executable instructions further comprise instructions that cause the barrier alarm device to transmit, via the transmitter, an immediate alarm signal to the receiver for causing a security response to be initiated when it is determined that the human detection device does not indicate that the human being is inside the premises in proximity to the barrier."** This claim is met by Lamb.

88. **Lamb discloses the processor-executable instructions further comprising instructions that cause the barrier alarm device** (*e.g.*, *see* [1.e]) **to transmit, via the transmitter** (*e.g.*, *see* [1.c])**, an immediate alarm signal to the receiver for causing a security response to be initiated when it is determined that the human detection device does not indicate that the human being is inside the premises in proximity to the barrier** (*e.g.*, "[w]hen the barrier alarm device

detects … that a human being is not inside the premises being monitored in proximity to the barrier, the barrier alarm device sends an alarm signal" "to central security panel 116"). *See*, *e.g.*, Lamb (emphasis added):

- **Fig. 5:**

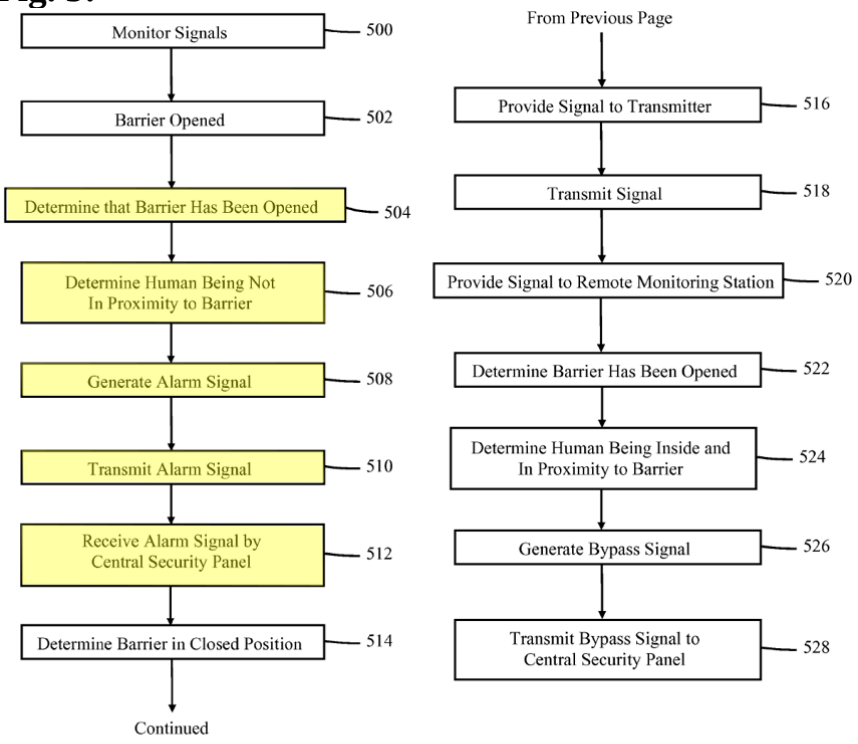


FIG. 5

FIG. 5
Continued

- **[0041]** ("*When the barrier alarm device detects that a barrier has been opened, and further that a human being is not inside the premises being monitored in proximity to the barrier, the barrier alarm device sends an alarm signal to gateway 402*, as this situation indicates that an unauthorized person outside the monitored premises has opened the barrier…. *The alarm signal may also be transmitted from the barrier alarm device to central security panel 116.*")
- **[0051]-[0053]** ("At block 508, *in response to determining that the barrier has been opened and that a human being is not inside the premises in proximity to the barrier, processor 300 generates an alarm signal and provides it to transmitter 308*. [¶] At block 510, *transmitter 308 transmits the alarm signal to receiver, such as central security panel 116*. Alternatively, or in addition, transmitter 308 transmits the alarm signal to

> gateway 402 connected to a wide area network, such as the Internet, for presentation to remote server 400. [¶] At block 512, *central security panel 116 receives the alarm signal from the barrier alarm device and takes at least one action*. For example, central security panel 116 may *cause a loud siren inside the premises to activate and/or send a remote alarm signal* to a remote monitoring station so that the remote monitoring station may summon appropriate authorities to the premises. Remote server 400 may also provide a notification to interested parties that an alarm signal was received.")

89. *See* my discussions for the elements of claim 1. As I discussed for claim element [1.f], **Lamb** discloses that the **barrier alarm device's processor 300** processes data that is received from the **barrier status detection device 306** (which comprises signals that indicate whether a door is open) and the **human detection device 304** (which comprises signals that indicate the presence of a person inside the premises proximate to the door). Lamb, [0037].

90. **Lamb** further discloses that its **barrier alarm device's processor 300** may, in different circumstances, determine that a door is open and then that a human is not inside the premises in proximity to the door. Lamb, [0037], [0041], [0051]-[0053]. **Lamb** discloses that in this case, the **processor 300** interprets this set of detections to indicate that an "unauthorized person" has opened the barrier and accordingly sends an "alarm signal" to the **central security panel 116**; this can cause, for example, the system to trigger a siren or contact the authorities without first initiating a timer. *Id.*

(j) Element [6.pre]

91. **Element [6.pre] recites "A central security panel, comprising."** This claim is met by Lamb in view of Williams.

92. **Lamb discloses a central security panel** (*e.g.*, "central security panel")**.** *See, e.g.*, Lamb (emphasis added):

- **Fig. 1:**

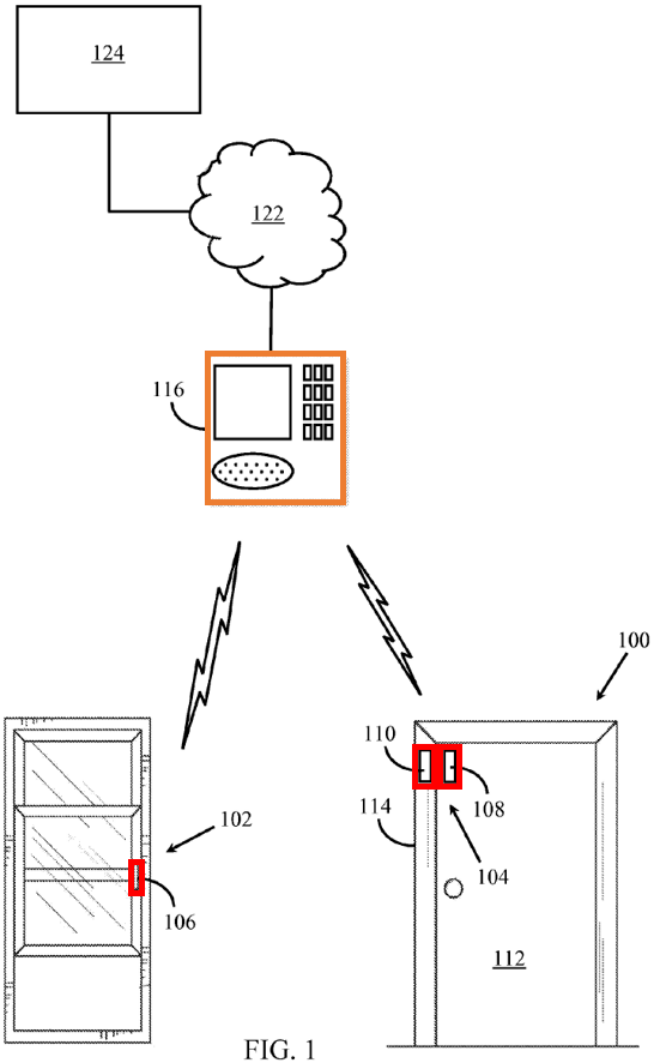


FIG. 1

- **[0020]** ("*Each of the barrier alarm devices communicates with receiver, such as central security panel 116, typically using wireless RF signals generated by the barrier alarm devices and/or central security panel 116.* For example, if door 112 is opened, reed switch assembly 110 detects a

reduction or elimination of a magnetic field produced by magnet 108 as magnet 108 moves away from reed switch assembly 110 as door 112 is opened. In response, reed switch assembly 110 transmits a message to central security panel 116 indicative of a local alarm condition, e.g., door 112 has been opened.")

- **[0036]** ("*Transmitter 308 comprises circuitry necessary to wirelessly transmit alarm signals and/or status messages and/or other information from the barrier alarm device to one or more receivers, such as central security panel 116 or a gateway device* coupled to a wide area network such as the Internet, either directly or through in intermediate device, such as a repeater, commonly used in popular mesh networks. Such circuitry is well known in the art and may comprise BlueTooth, Wi-Fi, RF, optical, ultrasonic circuitry, among others. Alternatively, or in addition, transmitter 308 comprises well-known circuitry to provide signals to central security panel 116 or a gateway via wiring, such as telephone wiring, twisted pair, two-conductor pair, CAT wiring, AC home wiring, or other type of wiring.")
- **[0037]** ("In any case, if processor 300 determines that a local alarm condition has occurred, *an alarm signal is provided to transmitter 308 for transmission to a remote location, such as central security panel 116 or a gateway*. In one embodiment, the alarm signal comprises a notification to central security panel 116 that a local alarm condition has been detected at a particular door or window being monitored by the barrier alarm device.")
- **[0041]** ("The alarm signal may also be *transmitted from the barrier alarm device to central security panel 116*.")

93. **Lamb** discloses "central security panel 116" for the same reasons as discussed for element [1.c]; namely, it explicitly discloses that its barrier alarm device includes a transmitter 308 component that can be used to transmit alarm signals to a central security panel 116.

(k) Element [6.a]

94. **Element [6.a] recites "a communication interface for receiving signals from a barrier alarm device." This claim is met by Lamb.**

95. **Lamb discloses a communication interface for receiving signals from a barrier alarm device** (*e.g.*, a receiver for receiving signals from a "barrier alarm device")**.** *See, e.g.*, Lamb (emphasis added):

- **Fig. 1:**

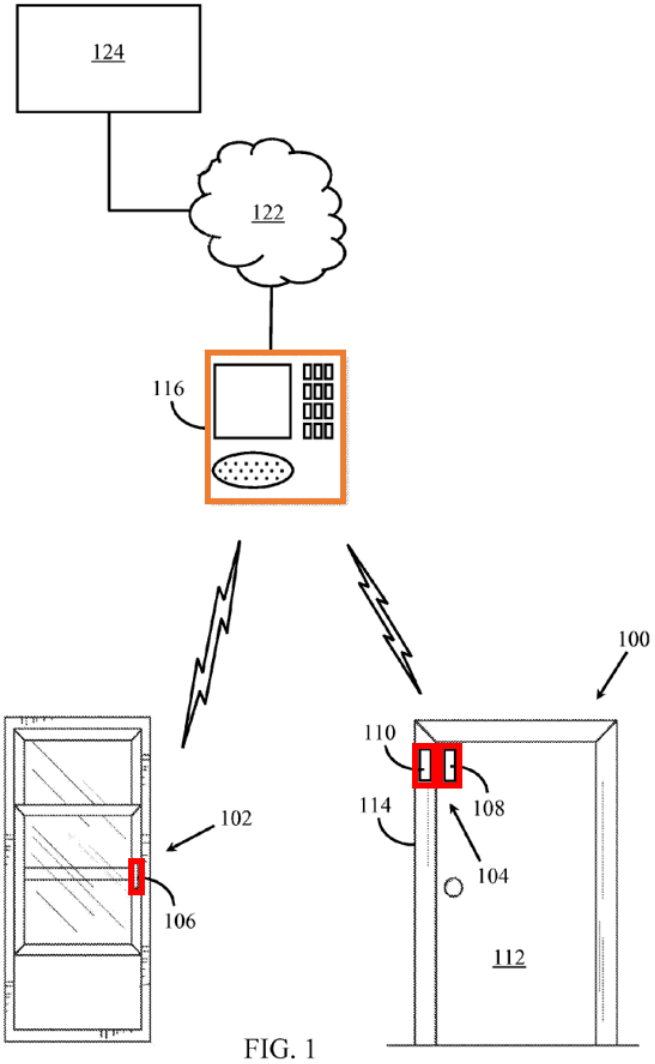


FIG. 1

- **Fig. 3:**

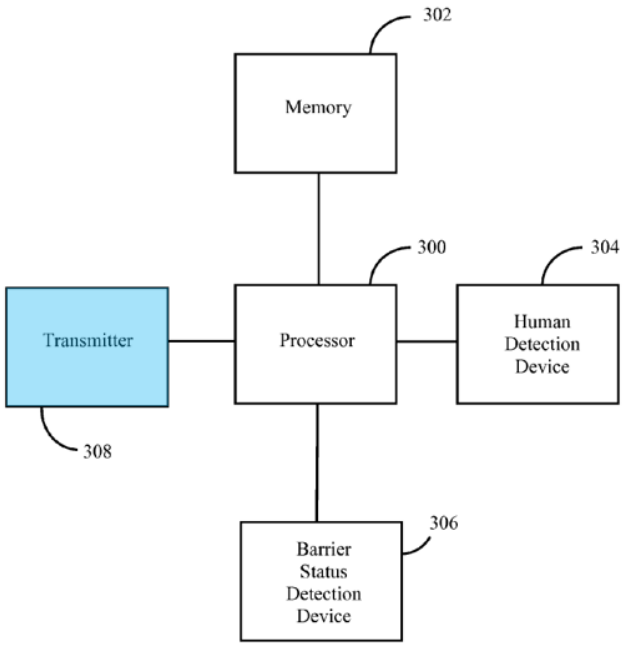


FIG. 3

- **[0020]** ("*Each of the barrier alarm devices communicates with receiver, such as central security panel 116, typically using wireless RF signals generated by the barrier alarm devices and/or central security panel 116.* For example, if door 112 is opened, reed switch assembly 110 detects a reduction or elimination of a magnetic field produced by magnet 108 as magnet 108 moves away from reed switch assembly 110 as door 112 is opened. In response, reed switch assembly 110 transmits a message to central security panel 116 indicative of a local alarm condition, e.g., door 112 has been opened.")
- **[0036]** ("*Transmitter 308 comprises circuitry necessary to wirelessly transmit alarm signals and/or status messages and/or other information from the barrier alarm device to one or more receivers, such as central security panel 116 or a gateway device* coupled to a wide area network such as the Internet, either directly or through in intermediate device, such as a repeater, commonly used in popular mesh networks. Such circuitry is well known in the art and may comprise BlueTooth, Wi-Fi, RF, optical, ultrasonic circuitry, among others. Alternatively, or in addition, transmitter 308 comprises well-known circuitry to provide signals to central security panel 116 or a gateway via wiring, such as telephone wiring, twisted pair, two-conductor pair, CAT wiring, AC home wiring, or other type of wiring.")

- **[0037]** ("In any case, if processor 300 determines that a local alarm condition has occurred, *an alarm signal is provided to transmitter 308 for transmission to a remote location, such as central security panel 116 or a gateway*. In one embodiment, the alarm signal comprises a notification to central security panel 116 that a local alarm condition has been detected at a particular door or window being monitored by the barrier alarm device.")
- **[0041]** ("The alarm signal may also be *transmitted from the barrier alarm device to central security panel 116*.")

96. *See* my discussion for elements [1.pre] and [1.c]. **Lamb** discloses that **central security panel 116** receives signals from a **barrier alarm device**. A person having ordinary skill in the art would have recognized that although **Lamb** does not *expressly* disclose **central security panel 116** including a "communication interface" for receiving signals from the **barrier alarm device**, a "communication interface" or "receiver" would have been necessary for the disclosed Wi-Fi, RF, and telephone communications. *See* [1.c].

(l) Element [6.b]

97. **Element [6.b] recites "a memory for storing processor-executable instructions."** This claim is met by Lamb.

98. **Lamb discloses a memory** (*e.g.*, "memory") **for storing processor-executable instructions.** *See*, *e.g.*, Lamb (emphasis added):

- **[0023]** ("In other embodiments, *central security panel 116 simply receives raw data from the barrier alarm devices and determines, based on the data, whether a local alarm condition has occurred*.")
- **[0043]** ("In another embodiment, barrier alarm device 106 does not make determinations as to when to transmit an alarm signal and/or a bypass signal. *Instead, processor 300* monitors barrier status determination device 306 and human detection device 304 and *transmits a barrier status signal and a*

human status signal, respectively, *to* gateway 402, *central security panel 116*, or both, *when a change in state of one or both devices occurs*. Remote server 400 and/or *central security panel 116 receives these status signals and determines whether a local alarm condition exists and whether to transmit an alarm signal to one or more remote devices 406 of interested parties and/or to a remote monitoring station 124*.")

99. *See* my discussion of elements [1.c]-[1.e]. **Lamb** discloses that its **barrier alarm device** is configured to store processor-executable instructions in its **memory 302** component, executing the instructions using its **processor 300** component, and transmit signals to **central security panel 116** using **transmitter 308**. *See* [1.c]-[1.e].

100. **Lamb** further discloses that **central security panel 116** may, instead of the **barrier alarm device**, be configured to "receive[] … status signals" from **processor 300** (which monitors barrier status determination device 306 and human detection device 304) and "make determinations" based on the status signals. Lamb, [0023], [0043]. While **Lamb** does not *expressly* disclose that **central security panel 116** includes memory and processor components that may be used to receive and process signals and make determinations based on these signals, a person having ordinary skill in the art would have appreciated that such a configuration would have necessary, or at least been obvious to include, to achieve Lamb's disclosed functionality. This is true at least in part because **Lamb** discloses **central security panel 116** as a partial replacement or alternative for that can perform some of the

functions of the **barrier alarm device**, which itself is configured with processor and memory components, and also because the reception and processing of such signals and data that are communicated over a network was well-known by a person having ordinary skill in the art to utilize memories and processors.

(m) Element [6.c]

101. **Element [6.c] recites "a processor coupled to the communication interface and the memory, for processing the processor-executable instructions that causes the central security panel to."** This claim is met by Lamb.

102. **Lamb discloses a processor coupled to the communication interface and the memory, for processing the processor-executable instructions** (*e.g.*, **).** *See, e.g.*, Lamb (emphasis added):

- **[0023]** ("In other embodiments, *central security panel 116 simply receives raw data from the barrier alarm devices and determines, based on the data, whether a local alarm condition has occurred*.")
- **[0043]** ("In another embodiment, barrier alarm device 106 does not make determinations as to when to transmit an alarm signal and/or a bypass signal. *Instead, processor 300* monitors barrier status determination device 306 and human detection device 304 and *transmits a barrier status signal and a human status signal*, respectively, *to* gateway 402, *central security panel 116*, or both, *when a change in state of one or both devices occurs*. Remote server 400 and/or *central security panel 116 receives these status signals and determines whether a local alarm condition exists and whether to transmit an alarm signal to one or more remote devices 406 of interested parties and/or to a remote monitoring station 124*.")

103. *See* my discussion of elements [6.a]-[6.b]. As I discussed for elements [6.a]-[6.b], **Lamb** discloses, and at least renders obvious, that **central security panel**

116 includes a communication interface that is used to receive signals from the **barrier alarm device** and a processor that executes processor-executable instructions that are stored in memory. Since **central security panel 116** receives signals from the **barrier alarm device** and also performs further processing to make determinations on how the security system should respond based on executable instructions, **Lamb** would have been understood by a person having ordinary skill in the art to disclose, and at least render obvious, that the processor is communicably coupled to the both the communications interface and memory components to facilitate the requisite access to signals and instructions.

(n) Element [6.d]

104. **Element [6.d] recites "receive a first alarm signal from a barrier alarm device that monitors a barrier of a premises, the first alarm signal indicative of the barrier being opened." This element is met by Lamb.**

105. **Lamb discloses the processor processing the processor-executable instructions** (*see* [6.c]) **to cause the central security panel to receive a first alarm signal from a barrier alarm device that monitors a barrier of a premises, the first alarm signal indicative of the barrier being opened** (*e.g.*, "[i]f … the authorized person … opens the barrier, barrier alarm device 106 transmits a barrier status signal to … central security panel 116")**.** *See, e.g.*, Lamb (emphasis added):

- **[0043]** ("If … the authorized person instead opens the barrier, *barrier alarm device 106 transmits a barrier status signal* to gateway 402, *central security panel 116*, or both, *indicative of the barrier being opened*.")

106. *See* my discussions for elements [1.a], [1.c], [1.f], and [6.a]-[6.c]. As I discussed for element [1.a], **Lamb** discloses that the **barrier alarm device's barrier detection device 306** monitors the position of a particular barrier and detects whether the barrier has been opened. *See* [1.a]. If the **barrier detection device 306** determines that the barrier it monitors has been opened, the **barrier alarm device** responds and "transmits a barrier status signal to … central security panel 116 … indicative of the barrier being opened." Lamb, [0043].

(o) Element [6.e]

107. **Element [6.e] recites "respond to the first alarm signal by determining whether a human being has been indicated to be inside the premises and in proximity to the barrier." This element is met by Lamb.**

108. **Lamb discloses the processor processing the processor-executable instructions** (*see* [6.c]-[6.d]) **to cause the central security panel to respond to the first alarm signal by determining whether a human being has been indicated to be inside the premises and in proximity to the barrier** (*e.g.*, responds to an indication of the barrier being opened by determining "the last known state of human detection device 304")**.** *See, e.g.*, Lamb (emphasis added):

- **[0043]** ("*If remote server 400 and/or central security panel 116 receives this status indication signal [of the barrier being opened], and the last known*

> *state of human detection device 304 is "person detected inside in proximity to barrier"*, then remote server 400 and/or central security panel 116 does not generate an alarm signal (but may provide a notification to interested parties of the status of the barrier such as "barrier open/authorized person present"). *If no authorized person was present when the human status signal was received indicating that the barrier had been opened*, remote server 400 and/or central security panel 116 generates an alarm signal that may provided to one or more interested parties and/or to remote monitoring station 124.")

109. *See* my discussion for elements [1.a]-[1.b], [1.f], and [6.d]. In addition, **Lamb** discloses that that **central security panel 116** responds to a signal indicating a barrier has been opened (as I discussed [6.d]) by then investigating whether a human is inside a premises in proximity to the barrier (as in [1.b], [1.f]) by determining the last known state of **human detection device 304**, which monitors this information. **Lamb** teaches that different actions may be taken depending on whether or not a human has been indicated by the system to be inside the premises; for example, the system may be directed to sound and alarm or bypass the alarm and ignore future alarm signals. Lamb, [0029].

(p) Element [6.f]

110. **Element [6.f] recites "begin a measuring of an elapsed time from when the first alarm signal was received when it is determined that the human being has been indicated to be inside the premises in proximity to the barrier."** This element is met by Lamb in view of Williams.

111. **Lamb discloses responding to a determination that the human being has been indicated to be inside the premises in proximity to the barrier** (*e.g.*, "[i]f … person detected inside in proximity to the barrier … provide a notification to interested parties of the status of the barrier"). *See, e.g.*, Lamb (emphasis added):

- **[0043]** ("*If … the last known state of human detection device 304 is "person detected inside in proximity to barrier", then* remote server 400 and/or *central security panel 116* … *may provide a notification* to interested parties of the status of the barrier such as "barrier open/authorized person present").

112. **Williams further discloses beginning a measuring of an elapsed time from when the first alarm signal was received when it is determined that the human being has been indicated to be inside the premises in proximity to the barrier** (*e.g.*, in response to receiving a signal when a human is detected, "control panel" initializes a timer that, upon timing out without receiving an authorized code, sets an alarm)**.** *See, e.g.*, Williams (emphasis added):

- **Fig. 2**

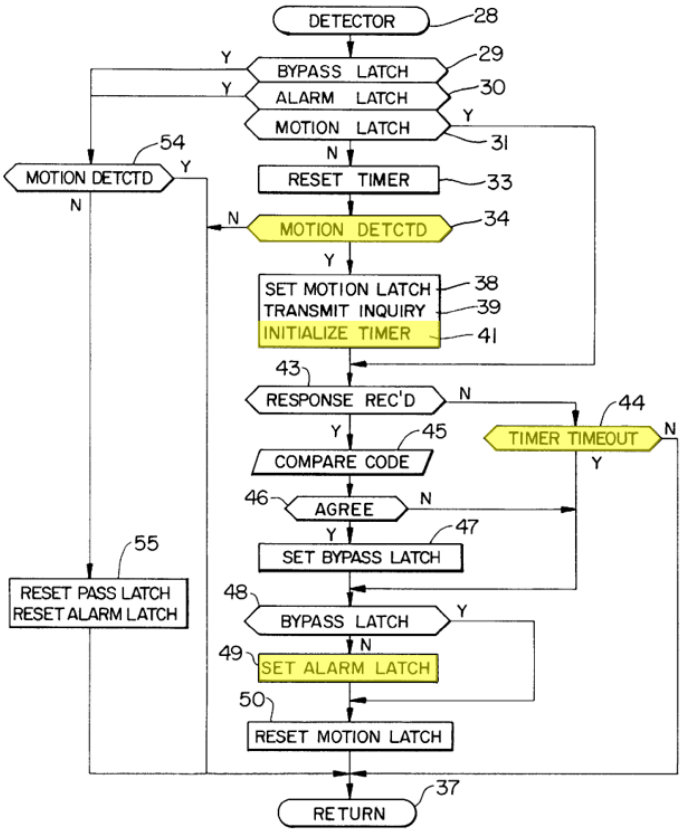


FIG. 2

- **Fig. 2A**

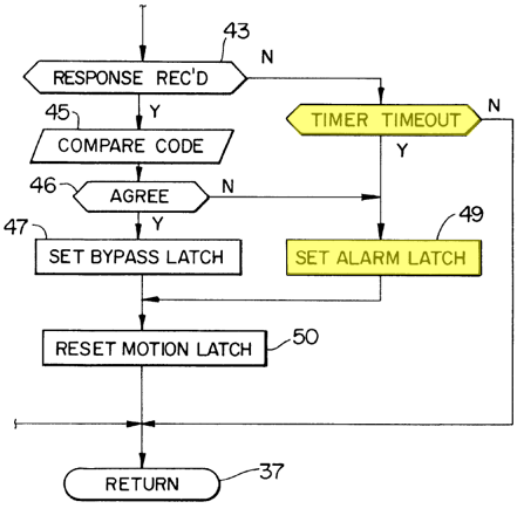


FIG. 2A

- **1:64-2:8** ("*[E]ach activation of a motion detector causes a corresponding transceiver to inquire*, by an electromagnetic transmission, *whether or not there is an authorized user in the space*, the portable device of the authorized user responding to the electromagnetic transmission with an appropriate code, *whereby a proper response will negate an alarm*.")
- **3:9-38** ("In operation, *should the motion detector for instance, sense motion of the person 20, an interrogation* by electromagnetic radiation … *will be received by the portable device 22, which in turn will respond with electromagnetic radiation … in like kind with the transmission of the motion detector 15, the transmission from the device 22 including a code to authenticate the authority of the user to be within the secure space while the alarm is on*…. Every possible switch or other sensor which could enter an alarm condition may similarly be provided with a transceiver, if desired…. For instance, *a transceiver within the control panel [17] may do the inquiry* for a potential alarm created by the switch 13 on the entry door 12 as well as *for a potential alarm created by motion within the room 10*. Suffice it to say that any potential alarm condition can be associated with a challenge for an authorization signal to cause the potential alarm condition to be deemed to not be a breach of the secure space.")
- **3:49-4:39** ("Referring now to FIG. 2, *a detector routine which performs the function of the invention with respect to a corresponding sensor, is reached through an entry point 28* and a first set of tests 29-31 determines if a pass latch, an alarm latch or a motion latch (described hereinafter) has been set or not. Prior to sensing motion, all three latches will not have been set, so negative results of tests 29-31 will reach a step 33 to reset a timer, as described more fully hereinafter. Then *a test 34 determines if the corresponding motion detector has detected motion*. … *[I]f motion has been detected, an affirmative result of test 34 will reach a step 38 to set the motion latch*, so that future passes through the routine of FIG. 2 will not go through the step 33 or the test 34, as described hereinafter. Then, *a step 39 causes an inquiry signal to be transmitted to determine if there is an authorized personal device within the proximity of the detector to which this routine relates*. And, *a step 41 initializes a timer to establish a period of time (perhaps a second or fraction thereof) within which an authorized response must be received*. [¶] *A test 43 determines if a response has been received, and if not, a negative result reaches a test 44 to determine if the timer, initialized in step 41, has timed out or not.* Initially, it may not, so a negative result of test 44 reaches the return point 37 to free-up the computer for other tasks. In the next pass through the routine of FIG. 2, tests 29 and 30

are still negative but test 31 is affirmative, returning the routine to test 43 to determine if a response has been received or not. *If a response has been received, an affirmative result of test 43 reaches a subroutine 45 to compare the authorization code within the response to the predetermined authorization code*…. *Then a test 46 determines if the two codes agree. If they do agree, an affirmative result of test 46 reaches a step 47 to set a bypass latch to indicate that this incidence of motion detection has responded to inquiry and has been authenticated.* Following comparison of the codes in the subroutine 45, if the test 46 is negative because the proper code was not received, the step 47 is bypassed. Then a test 48 determines if the bypass latch has been set or not; if not, an alarm latch is set in a step 49; but if the bypass latch is set, an affirmative result of test 48 avoids setting the alarm latch…. *On the other hand, if no response is received prior to time-out of the timer, the test 44 will be affirmative reaching the test 48 and the step 49 to similarly set the alarm latch. In other words, if a wrong code is received or no code is received, the alarm latch will be set in the step 49.* Thereafter, the step 50 will reset the motion latch to enable a future cycle of operation, and other programming is reverted to through the return point 37.")

- **7:43-63** ("*In any system which utilizes a warning sound and a delay in entering an alarm, as is typical at entry doors of conventional systems, then the present invention may be practiced by allowing the arming condition to go into effect, during which time if there is an authorized user, it will deactivate the alert condition causing the warning sound to cease and cancelling the alarm.*")
- **Claim 1** ("An alarm system comprising: one or more *motion detectors for providing a violation signal indicative of a potential alarm in response to sensing motion within a space*…")

113. As I discussed for elements [1.c] and [1.g], a person having ordinary skill in the art would have been motivated to modify **Lamb** to incorporate **Williams's** teaching of initializing a timer associated with the **central security panel** to enable verification that the potential alarm is indeed caused by an authorized person, as discussed in §VII.A.2. A person having ordinary skill in the

art would have understood that the Lamb system modified in this way would provide significantly greater protection to individuals in the premises by making conclusions about the authorization of the individual by actual verification, rather than assuming any person who is present is authorized.

114. As I discussed for elements [1.c] and [1.g], **Williams** discloses that a its system initializes a countdown timer upon determination of a circumstance that may trigger potential alarm (such as an open door or detected motion). Therefore, a person having ordinary skill in the art would have understood **Williams** to disclose that the control panel processor is configured to commence measurement of the time that has elapsed since it first detected that a human being was inside the premises in proximity to the barrier after determining that the barrier was open. Williams, 1:64-2:8, 3:19-38, 3:56-4:3, 4:12-27, 5:3-5.

115. To the extent this limitation could be interpreted as measuring the time that has elapsed starting at the time of receipt of the first alarm signal (that is, the signal that indicates that the barrier has been opened, as discussed for element [6.d]) and not measuring the time that has elapsed starting at the time of the determination that the human being is inside the premises (as discussed for element [6.e]; *see* '340, 2:30-36, 16:54-57, 21:22-32, 24:6-20), it would have been obvious to a person having ordinary skill in the art to measure either elapsed time based on **Lamb's** and **Williams's** disclosures. As I have previously discussed, **Lamb** discloses that once

it detects that the monitored barrier has been opened, this prompts the processor to check "the last known state of [the] human detection device." Lamb, [0043]. Because **Lamb** does not *require* a new reading from the human detection device upon determining that the barrier has been opened, a person having ordinary skill in the art would have understood that the difference between the time of receipt of the first alarm signal and the time of determination of the human being would have been negligible – the mere fractions of a second required to lookup "the last known state." Even if the human detection device were directed to acquire a new reading (which is *not* the sequence described by **Lamb**), the time to sense and transmit that data would be negligible in the described digital systems and/or, as further discussed below, accountable by a person having ordinary skill in the art designing a system with such "delay" in mind. Accordingly, a person having ordinary skill in the art would have recognized that, given **Williams'** teachings provide for the initialization of a timer in response to any potential alarm situation, measuring the time that has elapsed time from when a human being is detected would be substantially the same as, and therefore an obvious variation of, measuring the time that has elapsed from the receipt of the first alarm signal indicating the door has been opened.

116. A person having ordinary skill in the art would have also considered it obvious that the choice of which event should prompt timer initialization can be the detection of the first monitored condition (barrier status) or the second monitored

condition (human presence) because this is ultimately a design choice for implementing the system. Whether the timer is counted as, for example, 3 seconds or 3.5 seconds is an arbitrary difference, especially since **Williams** does not require the time period to be any particular length; **Williams** just suggests that an example time period may "perhaps" be one second. Williams, 3:67-4:3. A person having ordinary skill in the art would have been able to exercise ordinary creativity to balance the various system needs of security, speed, processing time, transmission time, and other factors to choose an arrive at an appropriate time period. For example, if a person having ordinary skill in the art sought to provide 5 seconds between detection of a potential alarm and a potential security response at the end of the 5 second, it may count 5 seconds from the last known condition to satisfy the potential alarm (*e.g.*, the presence of a human) or, alternatively, knowing that the system takes no longer than 0.1 seconds to process all conditions (*e.g.*, an open barrier and the presence of a human), it may count 5.1 seconds from the first condition met. The ability to account for these basic time considerations is well within the skill of a person having ordinary skill in the art. So long as the time period selected is long enough to receive an appropriate signal, it is arbitrary as to when the time period starts.

(q) Element [6.g]

117. **Element [6.g] recites "determine whether the elapsed time has exceeded a predetermined time."** This element is met by Lamb in view of Williams.

118. **Lamb in view of Williams renders obvious the processor processing the processor-executable instructions** (*see* [6.c]-[6.d]) **to cause the central security panel to determine whether the elapsed time has exceeded a predetermined time** (*e.g.*, determine a "time-out of the timer"). *See, e.g.*, Williams (emphasis added):

- **Fig. 2:**

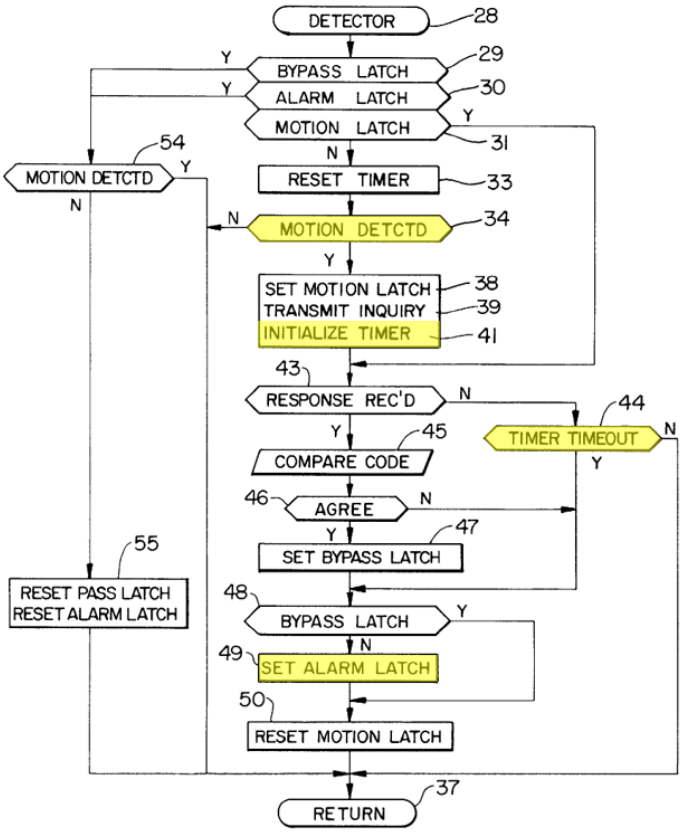


FIG. 2

- **Fig. 2A:**

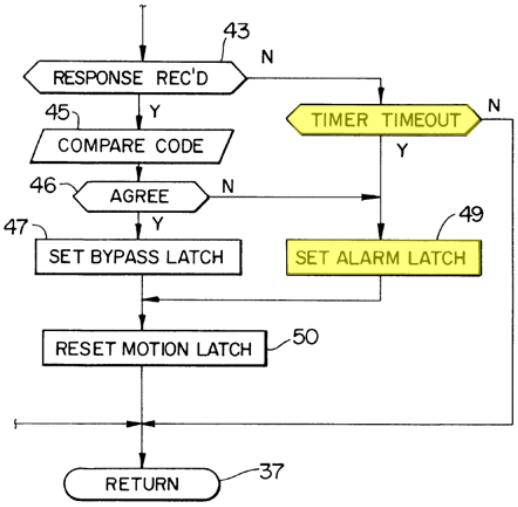


FIG. 2A

- **4:32-34** ("[I]f no response is received prior to *time-out of the timer*, … set the alarm latch.")

119. As I discussed for element [6.f], **Lamb** in view of **Williams** renders obvious the concept that the **central security panel** initializes a timer that sets an alarm once it elapses. **Williams** discloses that a "time-out of the timer" or "timer timeout" is determined after which the system "set[s] the alarm latch." Williams, Fig. 2A, 4:32-34.

(r) Element [6.h]

120. **Element [6.h] recites "generate a security response when it is determined that the elapsed time has exceeded the predetermined time."** This element is met by Lamb in view of Williams.

121. **Lamb in view of Williams renders obvious the processor processing the processor-executable instructions** (*see* [6.c]-[6.d]) **to cause the central security panel to generate a security response when it is determined that the elapsed time has exceeded the predetermined time** (*e.g.*, setting the alarm, notifying of the alarm, illuminating lights, sounding alerts). *See, e.g.*, Lamb (emphasis added):

122. **[0023]** ("When a local alarm condition is detected, *central security panel 116 generates a system alarm which may comprise taking one or more actions*, such as *notifying* remote monitoring station 124 that a local alarm condition has occurred, *illuminating* one or more lights, *sounding* one or more audible alerts, etc.")

123. **[0043]** ("Remote server 400 and/or central security panel 116 receives these status signals and determines whether a local alarm condition exists and whether to transmit an alarm signal to one or more remote devices 406 of interested parties and/or to a remote monitoring station 124.")

124. In addition, *see*, *e.g.*, Williams (emphasis added):

- **4:32-34** ("[I]f no response is received prior to *time-out of the timer*, … *set the alarm latch*.")

125. As I discussed for element [6.f], **Lamb** in view of **Williams** renders obvious the initialization of a timer by **central security panel** that upon expiration, sets an alarm. **Lamb** and **Williams** each disclose that an alarm condition is a security response; **Lamb** discloses various types of "system alarm[s]" and **Williams** provides an "alarm latch." Lamb, [0023]; Williams, 4:32-34.

(s) Element [6.i]

126. **Element [6.i] recites "provide the generated security response to a receiver via the communication interface."** This element is met by Lamb in view of Williams.

127. **Lamb in view of Williams renders obvious the processor processing the processor-executable instructions** (*see* [6.c]-[6.d]) **to cause the central security panel to provide the generated security response to a receiver via the communication interface** (*e.g.*, "transmit an alarm signal" to a remote station or

device of the alarm condition, via the communication interface). *See, e.g.*, Lamb (emphasis added):

- **[0023]** ("When a local alarm condition is detected, *central security panel 116 generates a system alarm which may comprise taking one or more actions*, such as *notifying* remote monitoring station 124 that a local alarm condition has occurred, *illuminating* one or more lights, *sounding* one or more audible alerts, etc.")
- **[0043]** ("Remote server 400 and/or *central security panel 116* receives these status signals and *determines whether a local alarm condition exists and whether to transmit an alarm signal to one or more remote devices 406 of interested parties and/or to a remote monitoring station 124*.")

128. As I discussed for element [6.f], **Lamb** in view of **Williams** renders obvious that the **central security panel** initializes a timer that sets an alarm if it is allowed to expire. **Lamb** discloses setting such an alarm by transmitting signals to "remote" devices and notifying others of the alarm condition. As I discussed for element [6.a], **central security panel 116** uses its communication interface to communicate with other devices using methods like "Wi-Fi." Lamb, [0036].

(t) Element [11.pre]

129. **Element [11.pre] recites "A method, comprising."** This element is met by Lamb.

130. **Lamb discloses a method** (*e.g.*, a "method"). *See, e.g.*, Lamb (emphasis added):

- [**0009]** ("[A] method … to reduce occurrences of false alarms….")
- ***See also* [0044], [0062]-[0064].**

131. Lamb explicitly discloses a method "to reduce occurrences of false alarms" in the context of a security system. Lamb, [0009].

(u) Element [11.a]

132. **Element [11.a] recites "in response to a barrier status detection device associated with a barrier alarm device indicating that a barrier being monitored by the barrier alarm device has been opened, determining whether a human detection device associated with the barrier alarm device indicates that a human being is inside a premises monitored by a central security panel in proximity to the barrier."** This claim is met by Lamb.

133. **Lamb discloses in response to a barrier status detection device associated with a barrier alarm device indicating that a barrier being monitored by the barrier alarm device has been opened, determining whether a human detection device associated with the barrier alarm device indicates that a human being is inside a premises monitored by a central security panel in proximity to the barrier** (*e.g.*, "[i]f processor 300 determines that a door or window has been opened, it checks to see whether human detection device 304 has sensed a person proximate to the barrier alarm device, door, or window," such as being "inside a monitored premises," *see* [1.f])**.** *See, e.g.*, Lamb (emphasis added):

- **Fig. 5:**

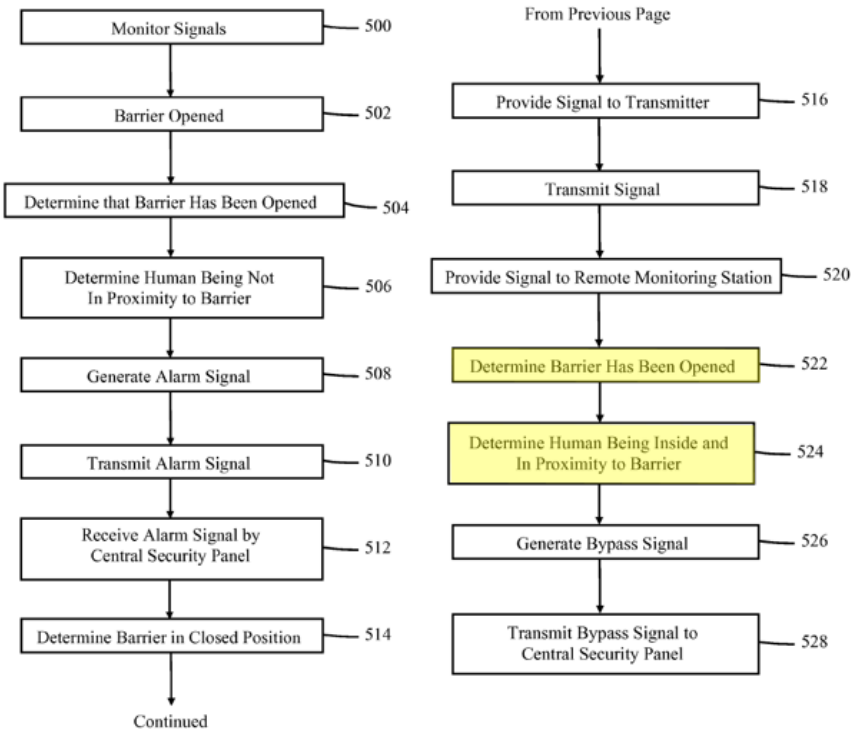


FIG. 5

FIG. 5
Continued

- **[0037]** ("In normal operation, processor 300 executes processor-executable instructions stored in memory 302 that causes *processor 300 to monitor signals provided by barrier status detection device 306 indicative of changes in one or more states*, physical conditions, attributes, status, or parameters of something being monitored, *such as the condition of a door or window being "open" or "closed"*, changes between these states, or simply "movement". *Processor 300 uses this data from barrier status detection device 306 to determine whether a predetermined condition has occurred relating to the barrier alarm device (herein "local alarm condition"), such as a door or window being monitored by the barrier alarm device changing state from "closed" to "open", movement between these states, or simply "movement".* Human detection device 304 monitors for the presence of a person proximate to the barrier alarm device, door or window and provides signals to processor 300 indicative of whether a human being is proximate or not. *If processor 300 determines that a door or window has been opened, it checks to see whether human detection device 304 has sensed a person proximate to the barrier alarm device, door, or window.…*. In any case, if processor 300 determines that a local alarm condition has occurred, an alarm signal is provided to transmitter 308 for transmission to a remote location,

such as central security panel 116 or a gateway. In one embodiment, the alarm signal comprises a notification to central security panel 116 that a local alarm condition has been detected at a particular door or window being monitored by the barrier alarm device.")

- **[0040]** ("In one embodiment, *when a barrier alarm device detects that a barrier, such as a door or a window, has been opened, and further that a human being is inside the premises being monitored in proximity to the barrier* … this situation indicates that an authorized person inside the monitored premises has opened the barrier.")
- **[0058]-[0059]** ("At block 522, after the barrier has been closed, *processor 300 determines that the barrier has been opened by detecting a change in a signal from barrier status detection device 306*. [¶] At block 524, *processor 300 determines that a human being is inside the premises in proximity to the barrier by evaluating the signals from human detection device 304*.")

134. **Lamb's** barrier alarm device that I discussed for the elements of claim 1, also transmits alarm signals to, and is consequently monitored by, a central security panel. The barrier alarm device is configured to perform a method that includes the same steps claimed in elements [11.a]-[12] that I will discuss now.

135. *See* my discussion of elements [1.e]-[1.f]. **Lamb** discloses that the **barrier alarm device's processor 300** processes data that it receives from the **barrier status detection device 306** (which include signals that indicate whether a door is open) and the **human detection device 304** (which include signals indicating a human is proximate to a door inside a premises). Lamb, [0037]. "[I]f" the **barrier status detection device 306** indicates that a door is "open," the **processor 300** then determines whether **human detection device 304** indicates that a human is inside a

premises. Lamb, [0037], [0040]. *See, e.g.*, steps 522 and 524. Lamb, Fig. 5, [0058]-[0059].

(v) Element [11.b]

136. **Element [11.b] recites "transmitting by the barrier alarm device a timed alarm signal to the central security panel for the purpose of initiating a timer associated with the central security panel only when it is determined that the human detection device indicates that the human being is in inside the premises and in proximity to the barrier."** This claim is met by Lamb in view of Williams.

137. **Lamb discloses transmitting by the barrier alarm device** (*e.g.*, transmit to the receiver associated with central security panel 116 (*see* [1.c])) **a timed alarm signal to the central security panel for the purpose of initiating a timer associated with the central security panel** (*e.g.*, for transmitting an alarm signal "to a remote location, such as central security panel 116" (*see* [1.c])) **only when it is determined that the human detection device indicates that the human being is in inside the premises and in proximity to the barrier** (*e.g.*, "when [the] barrier alarm device detects … that a human being is inside the premises being monitored in proximity to the barrier")**.** *See, e.g.*, Lamb (emphasis added):

- **Fig. 5:**

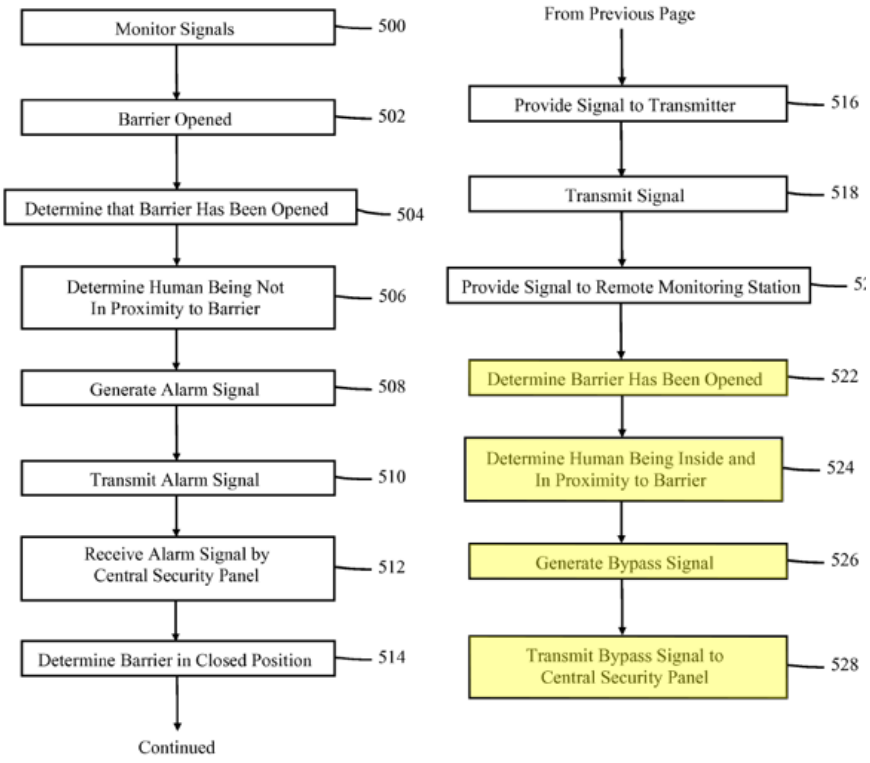


FIG. 5

FIG. 5
Continued

- **[0040]** ("In one embodiment, *when a barrier alarm device detects* that a barrier, such as a door or a window, has been opened, and further *that a human being is inside the premises being monitored in proximity to the barrier*, the barrier alarm device does not send an alarm signal to gateway 402, as *this situation indicates that an authorized person inside the monitored premises has opened the barrier*. In another embodiment, *a bypass signal is transmitted to central security panel 116*, as described above.")
- **[0060]** ("*At block 526, in response to determining that the barrier has been opened and that a human being is inside the premises in proximity to the barrier detection device*, processor 300 may refrain from sending an alarm signal to central security panel 116 and gateway 402. *Additionally, or alternatively, processor 300 generates a bypass signal and provides the bypass signal to transmitter 308 where it is transmitted to central security device 116 and/or gateway 402.* The bypass signal is an instruction to central security panel 116 to ignore future alarm signals generated by the barrier alarm device. The bypass signal may, additionally or alternatively, cause central security panel 116 to disarm the entire security system and to notify one or more persons that the security system has been disarmed, and/or that

> a barrier has been opened by an authorized person. Similarly, the bypass signal, or a different signal, may be transmitted to gateway 402 to provide an indication to remote server 400 that a barrier has been opened by an authorized person and to ignore future alarm signals generated by the barrier alarm device until the barrier is again placed into the closed position.")

- ***See also*** **[0037], [0050], [0058]-[0059].**

138. **Williams transmitting by the barrier alarm device a timed alarm signal to the central security panel for the purpose of initiating a timer associated with the central security panel only when it is determined that the human detection device indicates that the human being is inside the premises in proximity to the barrier** (*e.g.*, in response to receiving a signal when a human is detected, "control panel" initializes a timer that, upon timing out without receiving an authorized code, sets an alarm)**.** *See*, *e.g.*, Williams (emphasis added):

- **Fig. 2**

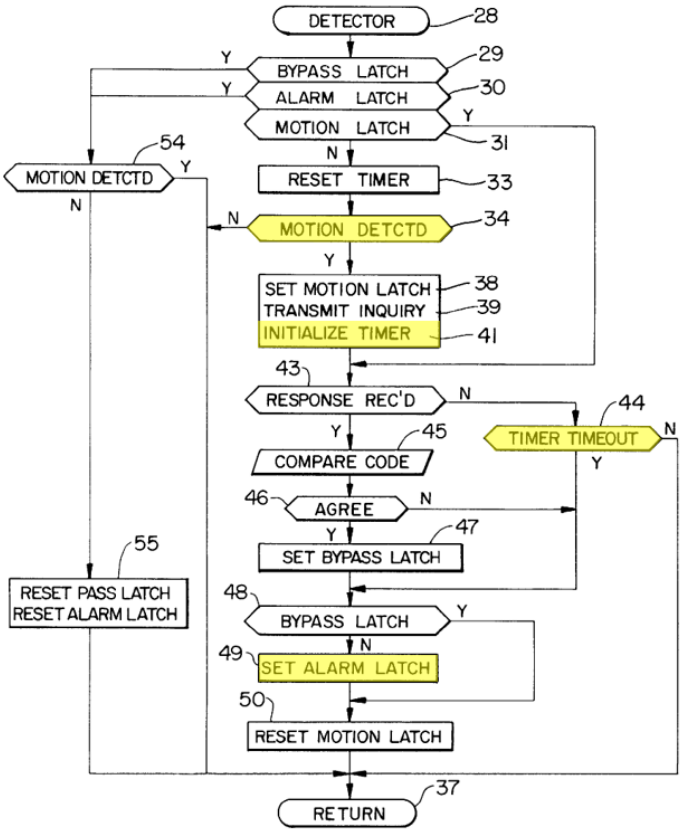


FIG. 2

- **Fig. 2A**

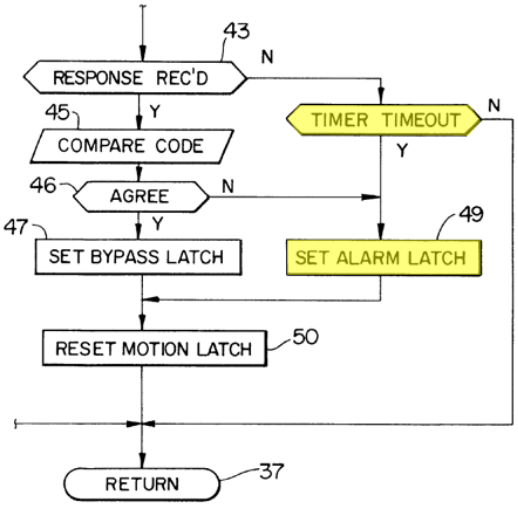


FIG. 2A

- **1:64-2:8** ("*[E]ach activation of a motion detector causes a corresponding transceiver to inquire*, by an electromagnetic transmission, *whether or not there is an authorized user in the space*, the portable device of the authorized user responding to the electromagnetic transmission with an appropriate code, *whereby a proper response will negate an alarm*.")
- **3:9-38** ("In operation, *should the motion detector for instance, sense motion of the person 20, an interrogation* by electromagnetic radiation … *will be received by the portable device 22, which in turn will respond with electromagnetic radiation … in like kind with the transmission of the motion detector 15, the transmission from the device 22 including a code to authenticate the authority of the user to be within the secure space while the alarm is on*…. Every possible switch or other sensor which could enter an alarm condition may similarly be provided with a transceiver, if desired…. For instance, *a transceiver within the control panel [17] may do the inquiry* for a potential alarm created by the switch 13 on the entry door 12 as well as *for a potential alarm created by motion within the room 10*. Suffice it to say that any potential alarm condition can be associated with a challenge for an authorization signal to cause the potential alarm condition to be deemed to not be a breach of the secure space.")
- **3:49-4:39** ("Referring now to FIG. 2, *a detector routine which performs the function of the invention with respect to a corresponding sensor, is reached through an entry point 28* and a first set of tests 29-31 determines if a pass latch, an alarm latch or a motion latch (described hereinafter) has been set or not. Prior to sensing motion, all three latches will not have been set, so negative results of tests 29-31 will reach a step 33 to reset a timer, as described more fully hereinafter. Then *a test 34 determines if the corresponding motion detector has detected motion*. … *[I]f motion has been detected, an affirmative result of test 34 will reach a step 38 to set the motion latch*, so that future passes through the routine of FIG. 2 will not go through the step 33 or the test 34, as described hereinafter. Then, *a step 39 causes an inquiry signal to be transmitted to determine if there is an authorized personal device within the proximity of the detector to which this routine relates*. And, *a step 41 initializes a timer to establish a period of time (perhaps a second or fraction thereof) within which an authorized response must be received*. [¶] *A test 43 determines if a response has been received, and if not, a negative result reaches a test 44 to determine if the timer, initialized in step 41, has timed out or not.* Initially, it may not, so a negative result of test 44 reaches the return point 37 to free-up the computer for other tasks. In the next pass through the routine of FIG. 2, tests 29 and 30

are still negative but test 31 is affirmative, returning the routine to test 43 to determine if a response has been received or not. *If a response has been received, an affirmative result of test 43 reaches a subroutine 45 to compare the authorization code within the response to the predetermined authorization code*…. *Then a test 46 determines if the two codes agree. If they do agree, an affirmative result of test 46 reaches a step 47 to set a bypass latch to indicate that this incidence of motion detection has responded to inquiry and has been authenticated.* Following comparison of the codes in the subroutine 45, if the test 46 is negative because the proper code was not received, the step 47 is bypassed. Then a test 48 determines if the bypass latch has been set or not; if not, an alarm latch is set in a step 49; but if the bypass latch is set, an affirmative result of test 48 avoids setting the alarm latch…. *On the other hand, if no response is received prior to time-out of the timer, the test 44 will be affirmative reaching the test 48 and the step 49 to similarly set the alarm latch. In other words, if a wrong code is received or no code is received, the alarm latch will be set in the step 49.* Thereafter, the step 50 will reset the motion latch to enable a future cycle of operation, and other programming is reverted to through the return point 37.")

- **7:43-63** ("*In any system which utilizes a warning sound and a delay in entering an alarm, as is typical at entry doors of conventional systems, then the present invention may be practiced by allowing the arming condition to go into effect, during which time if there is an authorized user, it will deactivate the alert condition causing the warning sound to cease and cancelling the alarm.*")
- **Claim 1** ("An alarm system comprising: one or more *motion detectors for providing a violation signal indicative of a potential alarm in response to sensing motion within a space*…")
- ***See also* Abstract, 2:11-18, Claims 5 and 8**

139. *See* my discussion for element [1.g]. **Lamb** teaches responding to a determination that a monitored door is open and that a human is present inside the premises proximate to the door with such actions as ignoring future alarm signals, disarming the system, and/or transmitting notifications regarding the open barrier and/or the status of the system to other parts of the system. Lamb, [0029], [0037],

[0040], [0050], [0058]-[0061]. As discussed in §VII.A.2. and [1.c] above, a person having ordinary skill in the art would have been motivated to modify **Lamb** to also include **Williams's** teaching of transmitting a timed alarm signal when the **barrier alarm device** detects that the monitored barrier has been opened and that a human is present within the relevant premises, providing time to verify the identity of the detected individual via an authorized user before triggering an alarm notification. **Williams** also discloses that potential alarms are created when motions of the barrier and humans are detected, and an appropriate code must be received within a certain time period (monitored by an initialized timer) to stop the setting of an alarm once the time period has elapsed. The signal causing the control panel to initiate this timed process would have been understood by a person having ordinary skill in the art to be a timed alarm signal. *See* [1.c].

(w) Claim [12]

140. **Claim [12] recites "The method of claim 11, further comprising transmitting by the barrier alarm device an immediate alarm signal to the central security panel for causing a security response to be initiated when it is determined that the human detection device does not indicate that the human being is in inside the premises and in proximity to the barrier."** This claim is met by Lamb.

141. **Lamb discloses transmitting by the barrier alarm device** (*e.g.*, *see* [1.c], [1.e]) **an immediate alarm signal to the central security panel for causing a security response to be initiated when it is determined that the human detection device does not indicate that the human being is in inside the premises and in proximity to the barrier** (*e.g.*, "[w]hen the barrier alarm device detects … that a human being is not inside the premises being monitored in proximity to the barrier, the barrier alarm device sends an alarm signal" "to central security panel 116")**.** *See*, *e.g.*, Lamb (emphasis added):

- **Fig. 5:**

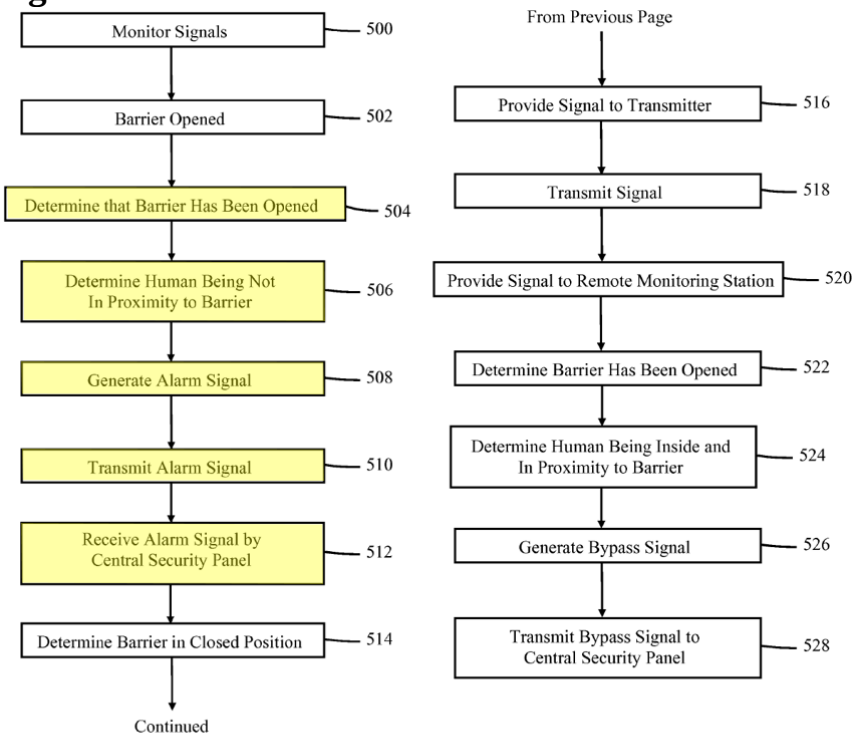


FIG. 5

FIG. 5
Continued

- **[0041]** ("*When the barrier alarm device detects that a barrier has been opened, and further that a human being is not inside the premises being monitored in proximity to the barrier, the barrier alarm device sends an*

alarm signal to gateway 402, as this situation indicates that an unauthorized person outside the monitored premises has opened the barrier…. *The alarm signal may also be transmitted from the barrier alarm device to central security panel 116.*")

- **[0051]-[0053]** ("At block 508, *in response to determining that the barrier has been opened and that a human being is not inside the premises in proximity to the barrier, processor 300 generates an alarm signal and provides it to transmitter 308*. [¶] At block 510, *transmitter 308 transmits the alarm signal to receiver, such as central security panel 116*. Alternatively, or in addition, transmitter 308 transmits the alarm signal to gateway 402 connected to a wide area network, such as the Internet, for presentation to remote server 400. [¶] At block 512, *central security panel 116 receives the alarm signal from the barrier alarm device and takes at least one action*. For example, central security panel 116 may *cause a loud siren inside the premises to activate and/or send a remote alarm signal* to a remote monitoring station so that the remote monitoring station may summon appropriate authorities to the premises. Remote server 400 may also provide a notification to interested parties that an alarm signal was received.")

142. *See* my discussions for the elements of claims 1, 2, and 11. As I discussed for claim [2], **Lamb** discloses that the **barrier alarm device's processor 300** processes data that is received from the **barrier status detection device 306** (which comprises signals that indicate whether a door is open) and the **human detection device 304** (which comprises signals that indicate the presence of a person inside the premises proximate to the door). Lamb, [0037].

143. **Lamb** further discloses that when its **barrier alarm device** determines that a door is open and then that a human is not inside the premises in proximity to the door, the **processor 300** interprets this set of detections to indicate that an

"unauthorized person" has opened the barrier and accordingly sends an "alarm signal" to the **central security panel 116**. Lamb, [0037], [0041], [0051]-[0053].

(x) Element [16.pre]

144. **Element [16.pre] recites "A central security panel, comprising."** This claim is met by Lamb.

145. **Lamb discloses a central security panel** (*e.g.*, "central security panel")**.** *See, e.g.*, Lamb (emphasis added):

- **Fig. 1:**

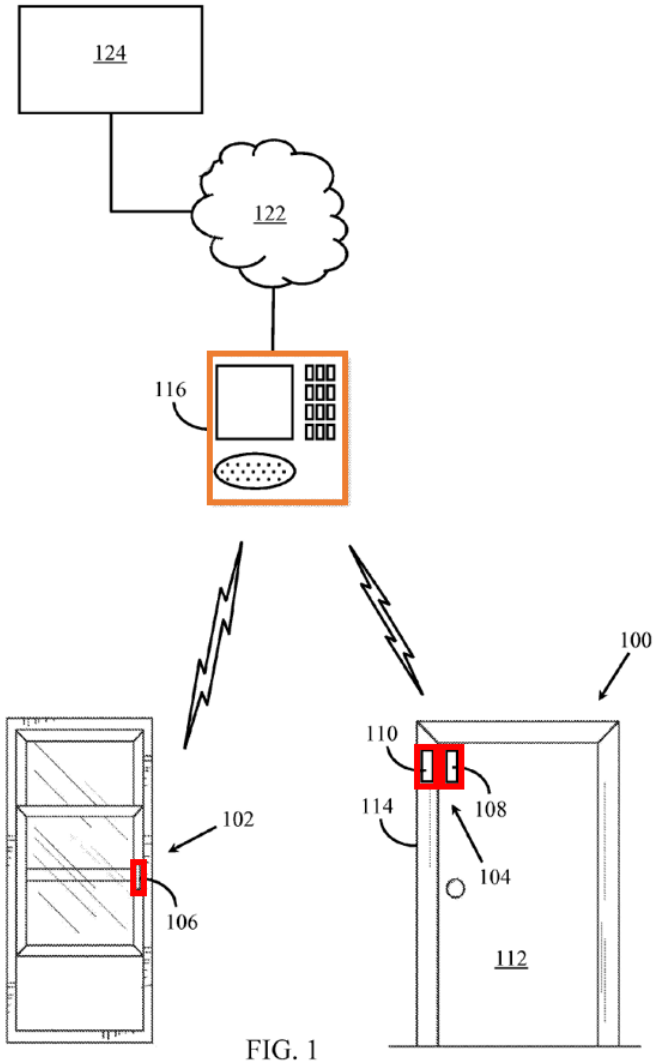


FIG. 1

- **[0020]** ("*Each of the barrier alarm devices communicates with receiver, such as central security panel 116, typically using wireless RF signals generated by the barrier alarm devices and/or central security panel 116.* For example, if door 112 is opened, reed switch assembly 110 detects a reduction or elimination of a magnetic field produced by magnet 108 as magnet 108 moves away from reed switch assembly 110 as door 112 is opened. In response, reed switch assembly 110 transmits a message to central security panel 116 indicative of a local alarm condition, e.g., door 112 has been opened.")
- **[0036]** ("*Transmitter 308 comprises circuitry necessary to wirelessly transmit alarm signals and/or status messages and/or other information from the barrier alarm device to one or more receivers, such as central security panel 116 or a gateway device* coupled to a wide area network such as the Internet, either directly or through in intermediate device, such as a repeater, commonly used in popular mesh networks. Such circuitry is well known in the art and may comprise BlueTooth, Wi-Fi, RF, optical, ultrasonic circuitry, among others. Alternatively, or in addition, transmitter 308 comprises well-known circuitry to provide signals to central security panel 116 or a gateway via wiring, such as telephone wiring, twisted pair, two-conductor pair, CAT wiring, AC home wiring, or other type of wiring.")
- **[0037]** ("In any case, if processor 300 determines that a local alarm condition has occurred, *an alarm signal is provided to transmitter 308 for transmission to a remote location, such as central security panel 116 or a gateway*. In one embodiment, the alarm signal comprises a notification to central security panel 116 that a local alarm condition has been detected at a particular door or window being monitored by the barrier alarm device.")
- **[0041]** ("The alarm signal may also be *transmitted from the barrier alarm device to central security panel 116*.")

146. **Lamb** discloses a "central security panel" for the same reasons as discussed for element [1.c]; Lamb explicitly describes a "central security panel 116."

(y) Element [16.a]

147. **Element [16.a] recites "receiving a first alarm signal from a barrier alarm device that monitors a barrier of a premises, the first alarm signal indicative of the barrier being opened." This element is met by Lamb.**

148. **Lamb discloses receiving a first alarm signal from a barrier alarm device that monitors a barrier of a premises, the first alarm signal indicative of the barrier being opened** (*e.g.*, "[i]f … the authorized person … opens the barrier, barrier alarm device 106 transmits a barrier status signal to … central security panel 116" (*see* [6.d])**.** *See, e.g.*, Lamb (emphasis added):

- **[0043]** ("If … the authorized person instead opens the barrier, *barrier alarm device 106 transmits a barrier status signal* to gateway 402, *central security panel 116*, or both, *indicative of the barrier being opened*.")

149. *See* my discussions for elements [1.a], [1.c], [1.f], and [6.a]-[6.d]. **Lamb** discloses that the **barrier alarm device's barrier detection device 306** monitors the position of a particular barrier and detects whether the barrier has been opened. *See* [1.a]. If the **barrier detection device 306** determines that the barrier it monitors has been opened, the **barrier alarm device** responds and "transmits a barrier status signal to … central security panel 116 … indicative of the barrier being opened." Lamb, [0043].

(z) Element [16.b]

150. **Element [16.b] recites "responding to the first alarm signal by determining whether a human being has been indicated to be inside the premises in proximity to the barrier." This element is met by Lamb.**

151. **Lamb discloses responding to the first alarm signal by determining whether a human being has been indicated to be inside the premises in**

proximity to the barrier (*e.g.*, responds to an indication of the barrier being opened by determining "the last known state of human detection device 304" (*see* [6.e])**.**

See, e.g., Lamb (emphasis added):

- **[0043]** ("*If remote server 400 and/or central security panel 116 receives this status indication signal [of the barrier being opened], and the last known state of human detection device 304 is "person detected inside in proximity to barrier"*, then remote server 400 and/or central security panel 116 does not generate an alarm signal (but may provide a notification to interested parties of the status of the barrier such as "barrier open/authorized person present"). *If no authorized person was present when the human status signal was received indicating that the barrier had been opened*, remote server 400 and/or central security panel 116 generates an alarm signal that may provided to one or more interested parties and/or to remote monitoring station 124.")

152. *See* my discussion for elements [1.a]-[1.b], [1.f], and [6.d]-[6.e]. In addition, **Lamb** discloses that that **central security panel 116** responds to a signal indicating a barrier has been opened (as I discussed [6.d]) by then investigating whether a human is inside a premises in proximity to the barrier (as in [1.b], [1.f]) by determining the last known state of **human detection device 304**, which monitors this information. **Lamb** teaches that different actions may be taken depending on whether or not a human has been indicated by the system to be inside the premises; for example, the system may be directed to sound and alarm or bypass the alarm and ignore future alarm signals. Lamb, [0029].

(aa) Element [16.c]

153. **Element [16.c] recites "starting a countdown timer when it is determined that the human being has been indicated to be inside the premises in proximity to the barrier."** This element is met by Lamb in view of Williams.

154. **Lamb discloses responding after it is determined that the human being has been indicated to be inside the premises in proximity to the barrier** (*e.g.*, "[i]f … person detected inside in proximity to the barrier … provide a notification to interested parties of the status of the barrier"). *See, e.g.*, Lamb (emphasis added):

- **[0043]** ("*If … the last known state of human detection device 304 is "person detected inside in proximity to barrier", then* remote server 400 and/or *central security panel 116* … *may provide a notification* to interested parties of the status of the barrier such as "barrier open/authorized person present").

155. **Williams further discloses starting a countdown timer when it is determined that the human being has been indicated to be inside the premises in proximity to the barrier** (*e.g.*, in response to receiving a signal when a human is detected, "control panel" initializes a timer that, upon timing out without receiving an authorized code, sets an alarm)**.** *See, e.g.*, Williams (emphasis added):

- **Fig. 2**

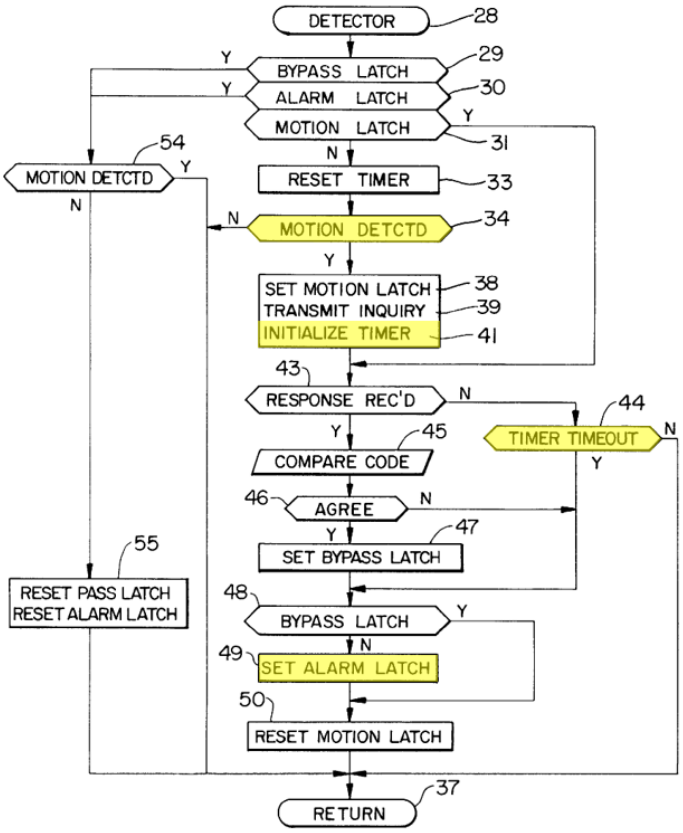


FIG. 2

- **Fig. 2A**

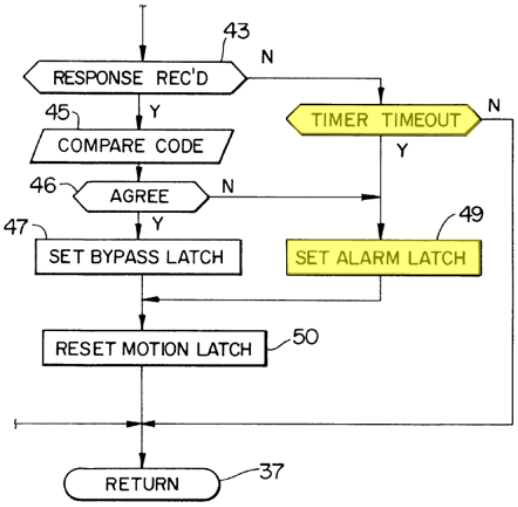


FIG. 2A

- **1:64-2:8** ("*[E]ach activation of a motion detector causes a corresponding transceiver to inquire*, by an electromagnetic transmission, *whether or not there is an authorized user in the space*, the portable device of the authorized user responding to the electromagnetic transmission with an appropriate code, *whereby a proper response will negate an alarm*.")
- **3:9-38** ("In operation, *should the motion detector for instance, sense motion of the person 20, an interrogation* by electromagnetic radiation … *will be received by the portable device 22, which in turn will respond with electromagnetic radiation … in like kind with the transmission of the motion detector 15, the transmission from the device 22 including a code to authenticate the authority of the user to be within the secure space while the alarm is on*…. Every possible switch or other sensor which could enter an alarm condition may similarly be provided with a transceiver, if desired…. For instance, *a transceiver within the control panel [17] may do the inquiry* for a potential alarm created by the switch 13 on the entry door 12 as well as *for a potential alarm created by motion within the room 10*. Suffice it to say that any potential alarm condition can be associated with a challenge for an authorization signal to cause the potential alarm condition to be deemed to not be a breach of the secure space.")
- **3:49-4:39** ("Referring now to FIG. 2, *a detector routine which performs the function of the invention with respect to a corresponding sensor, is reached through an entry point 28* and a first set of tests 29-31 determines if a pass latch, an alarm latch or a motion latch (described hereinafter) has been set or not. Prior to sensing motion, all three latches will not have been set, so negative results of tests 29-31 will reach a step 33 to reset a timer, as described more fully hereinafter. Then *a test 34 determines if the corresponding motion detector has detected motion*. … *[I]f motion has been detected, an affirmative result of test 34 will reach a step 38 to set the motion latch*, so that future passes through the routine of FIG. 2 will not go through the step 33 or the test 34, as described hereinafter. Then, *a step 39 causes an inquiry signal to be transmitted to determine if there is an authorized personal device within the proximity of the detector to which this routine relates*. And, *a step 41 initializes a timer to establish a period of time (perhaps a second or fraction thereof) within which an authorized response must be received*. [¶] *A test 43 determines if a response has been received, and if not, a negative result reaches a test 44 to determine if the timer, initialized in step 41, has timed out or not.* Initially, it may not, so a negative result of test 44 reaches the return point 37 to free-up the computer for other tasks. In the next pass through the routine of FIG. 2, tests 29 and 30

are still negative but test 31 is affirmative, returning the routine to test 43 to determine if a response has been received or not. *If a response has been received, an affirmative result of test 43 reaches a subroutine 45 to compare the authorization code within the response to the predetermined authorization code*…. *Then a test 46 determines if the two codes agree. If they do agree, an affirmative result of test 46 reaches a step 47 to set a bypass latch to indicate that this incidence of motion detection has responded to inquiry and has been authenticated.* Following comparison of the codes in the subroutine 45, if the test 46 is negative because the proper code was not received, the step 47 is bypassed. Then a test 48 determines if the bypass latch has been set or not; if not, an alarm latch is set in a step 49; but if the bypass latch is set, an affirmative result of test 48 avoids setting the alarm latch…. *On the other hand, if no response is received prior to time-out of the timer, the test 44 will be affirmative reaching the test 48 and the step 49 to similarly set the alarm latch. In other words, if a wrong code is received or no code is received, the alarm latch will be set in the step 49.* Thereafter, the step 50 will reset the motion latch to enable a future cycle of operation, and other programming is reverted to through the return point 37.")

- **7:43-63** ("*In any system which utilizes a warning sound and a delay in entering an alarm, as is typical at entry doors of conventional systems, then the present invention may be practiced by allowing the arming condition to go into effect, during which time if there is an authorized user, it will deactivate the alert condition causing the warning sound to cease and cancelling the alarm.*")
- **Claim 1** ("An alarm system comprising: one or more *motion detectors for providing a violation signal indicative of a potential alarm in response to sensing motion within a space*…")

156. Lamb discloses this element for the same reasons discussed for element [6.e]. **Lamb** discloses that that **central security panel 116** responds to a signal indicating a barrier has been opened (as I discussed for element [6.d]) by then investigating whether a human is inside a premises in proximity to the barrier (as in [1.b], [1.f]) by determining the last known state of **human detection device 304**,

which monitors this information. **Lamb** teaches that different actions may be taken depending on whether or not a human has been indicated by the system to be inside the premises; for example, the system may be directed to sound and alarm or bypass the alarm and ignore future alarm signals. Lamb, [0029].

(bb) Element [16.d]

157. **Element [16.d] recites "determining whether the countdown timer has expired."** This element is met by Lamb in view of Williams.

158. **Lamb in view of Williams renders obvious determining whether the countdown timer has expired** (*e.g.*, determine a "time-out of the timer"). *See, e.g.*, Williams (emphasis added):

- **Fig. 2:**

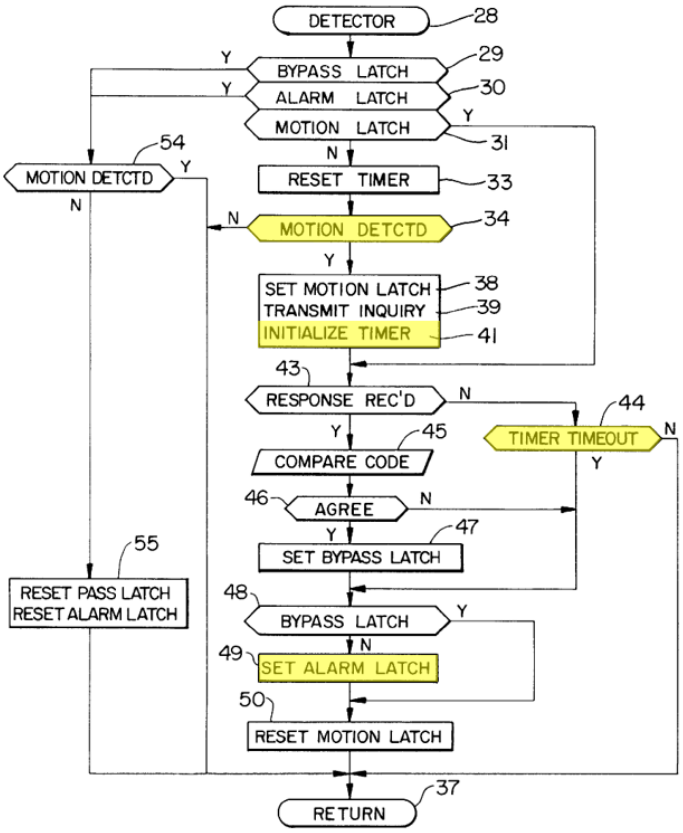


FIG. 2

- **Fig. 2A:**

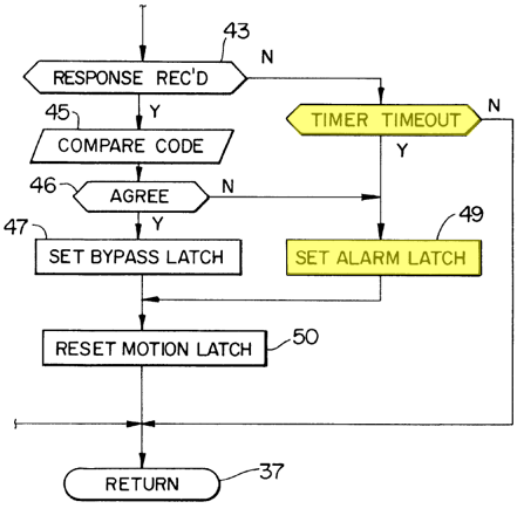


FIG. 2A

- **4:32-34** ("[I]f no response is received prior to *time-out of the timer*, … set the alarm latch.")

159. As I discussed for element [6.f], **Lamb** in view of **Williams** renders obvious that the **central security panel** initializes a timer that prompts the setting of an alarm once it expires. **Williams** discloses determining a "time-out of the timer" or a "timer timeout." While this element recites a "countdown timer," a person having ordinary skill in the art would have understood that this "countdown timer" performs the same functionality as the measurement of an elapsed time claimed in element [6.f], since both monitor the amount of time that has passed since a relevant event that prompted a timed alarm signal.

(cc) Element [16.e]

160. **Element [16.e] recites "in response to determining that the countdown timer has expired, generating a security response."** This element is met by Lamb in view of Williams.

161. **Lamb in view of Williams renders obvious in response to determining that the countdown timer has expired, generating a security response** (*e.g.*, setting the alarm, notifying of the alarm, illuminating lights, sounding alerts). *See*, *e.g.*, Lamb (emphasis added):

162. **[0023]** ("When a local alarm condition is detected, *central security panel 116 generates a system alarm which may comprise taking one or more actions*,

such as *notifying* remote monitoring station 124 that a local alarm condition has occurred, *illuminating* one or more lights, *sounding* one or more audible alerts, etc.")

163. **[0043]** ("Remote server 400 and/or central security panel 116 receives these status signals and determines whether a local alarm condition exists and whether to transmit an alarm signal to one or more remote devices 406 of interested parties and/or to a remote monitoring station 124.")

164. In addition, *see, e.g.*, Williams (emphasis added):

- **4:32-34** ("[I]f no response is received prior to *time-out of the timer*, … *set the alarm latch*.")

165. This element is disclosed for the same reasons I discussed for element [6.h]. **Lamb** in view of **Williams** renders obvious that the **central security panel** initializes a timer that sets an alarm after it expires. **Lamb** and **Williams** each disclose that an alarm condition is a security response. While this element recites a "countdown timer," a person having ordinary skill in the art would have understood that this "countdown timer" performs the same functionality as the measurement of an elapsed time claimed in element [6.g], since both monitor the amount of time that has passed since a relevant event that prompted a timed alarm signal.

(dd) Element [16.f]

166. **Element [16.f] recites "providing the generated security response to a receiver via a communication interface."** This element is met by Lamb in view of Williams.

167. **Lamb in view of Williams renders obvious providing the generated security response to a receiver via a communication interface** (*e.g.*, "transmit an alarm signal" to a remote station or device of the alarm condition, via the communication interface)**.** *See*, *e.g.*, Lamb (emphasis added):

- **[0023]** ("When a local alarm condition is detected, *central security panel 116 generates a system alarm which may comprise taking one or more actions*, such as *notifying* remote monitoring station 124 that a local alarm condition has occurred, *illuminating* one or more lights, *sounding* one or more audible alerts, etc.")
- **[0043]** ("Remote server 400 and/or *central security panel 116* receives these status signals and *determines whether a local alarm condition exists and whether to transmit an alarm signal to one or more remote devices 406 of interested parties and/or to a remote monitoring station 124*.")

168. This element is met for the same reasons discussed for element [6.i]. **Lamb** in view of **Williams** renders obvious that the **central security panel** initializes a timer that sets an alarm after it expires. **Lamb** discloses transmitting signals to "remote" devices to notify them of an alarm condition triggered by the system. As discussed for [6.a], **central security panel 116** communicates with the communication interface with other devices that are part of the system using, for example "Wi-Fi." Lamb, [0036].

B. Ground 2: Sharma (Claims 1 and 11)

1. U.S. 7,696,873 ("Sharma") Overview

169. **Sharma** discloses automatically arming and disarming a barrier alarm in the context of a security system. Sharma teaches that a **door sensing unit 104**

"installed proximate to the **first door 112**." Sharma, 5:63-64. The **door sensing unit 104** comprises a **door contact 172** and a **motion detector 174**, as well as other components,. Sharma, 4:50-51. Figures 1 and 2 from Sharma below (annotated) indicating the relevant components.

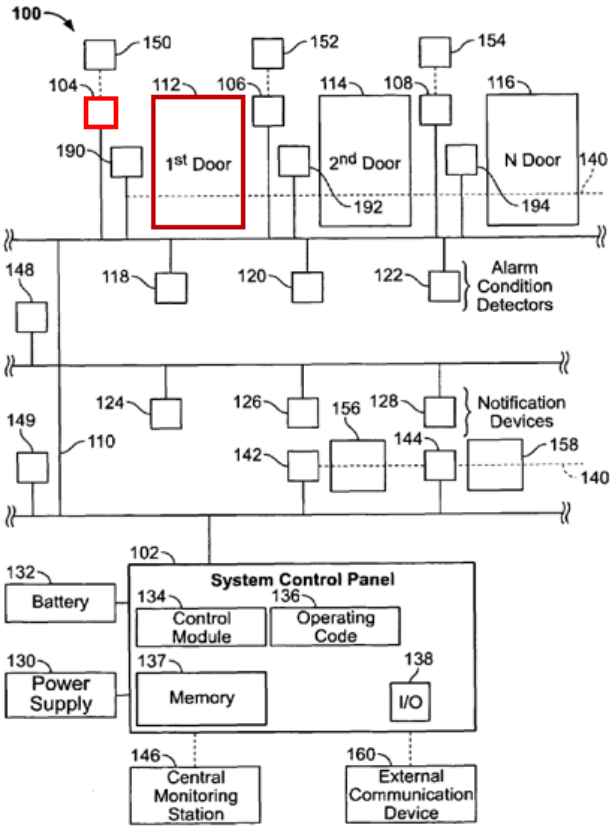


FIG. 1

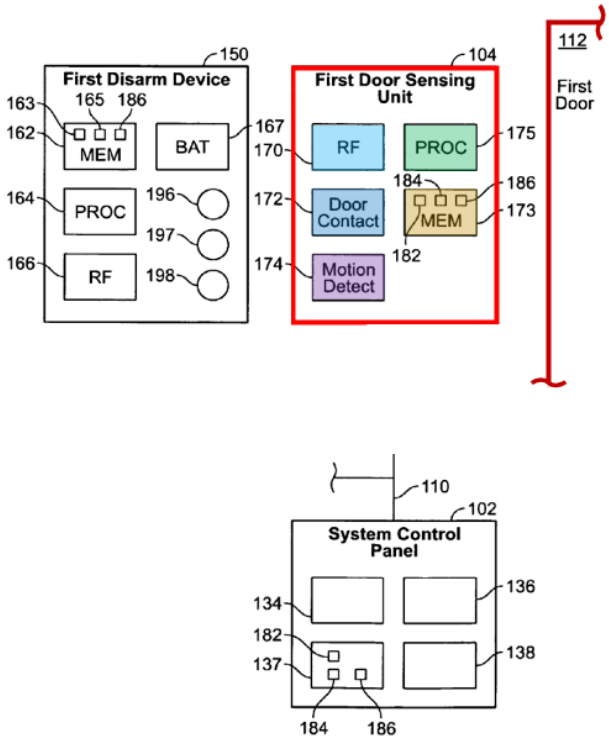


FIG. 2

Door contact 172 is used to detect whether the **first door 112** is open or closed. 4:51-53. **Motion detector 174** senses motion "proximate to the inside of first door 112," which a person having ordinary skill in the art would have understood to be intended primarily to detect human motion. Sharma, 4:53-56.

170. Figure 5 demonstrates how the device operates:

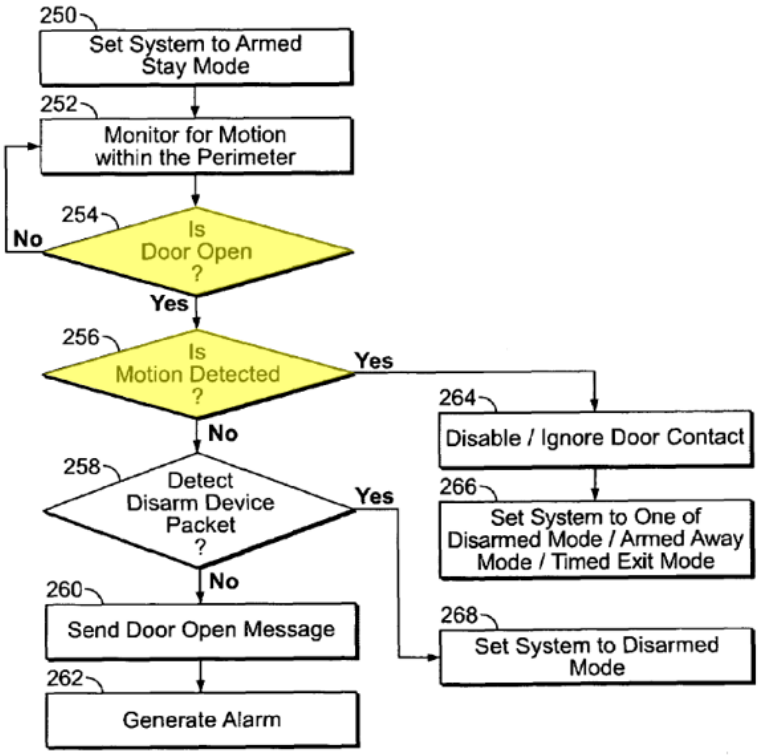


FIG. 5

At step **250**, the system is set into Armed Stay mode which activates the door sensor units to monitor their respective **first doors**. Sharma, 7:38-42. At **252**, **motion detector 174** activates and monitors the area proximate to the inside of the monitored **first door 112** for motion, although on its own, the detection of motion will not trigger any alarm. Sharma, 7:47-51. At step **254**, **door sensing unit 104's processor 175** uses signals from **door contact 172** to determine whether the **door** is open. Sharma, 7:52-54. If the **door** is open, then at step **256**, the **processor 175** next determines whether **motion detector 174** detects motion proximate to the open **barrier**. Sharma, 7:56-58. If motion is detected, then at step **264**, **processor 175** disables the **door contact 172** and/or ignores the door open message from **door**

contact 172. Sharma, 8:1-5. After this, at step 266, **processor 175** sends a signal to **system control panel 102** to change the status of the system; the status may be changes to any of, for example, a "Disarmed Mode" where an alarm is not triggered in response to detected motion, an "Armed Away Mode" where an alarm will be triggered, or a "Timed Exit Mode" that "allows people to leave the house or facility without having to interact with the system 100." Sharma, 8:6-21. After a predetermined time, the system is reset. Sharma, 8:13-18.

2. Invalidity of Claims 1 and 11 Over Sharma

(a) Element [1.pre]

171. **Element [1.pre] recites "A barrier alarm device, comprising."** This element is met by Sharma.

172. **Sharma discloses a barrier alarm device** (*e.g.*, "door sensing unit" can generate an alarm)**.** *See*, *e.g.*, Sharma (emphasis added):

- **Fig. 1:**

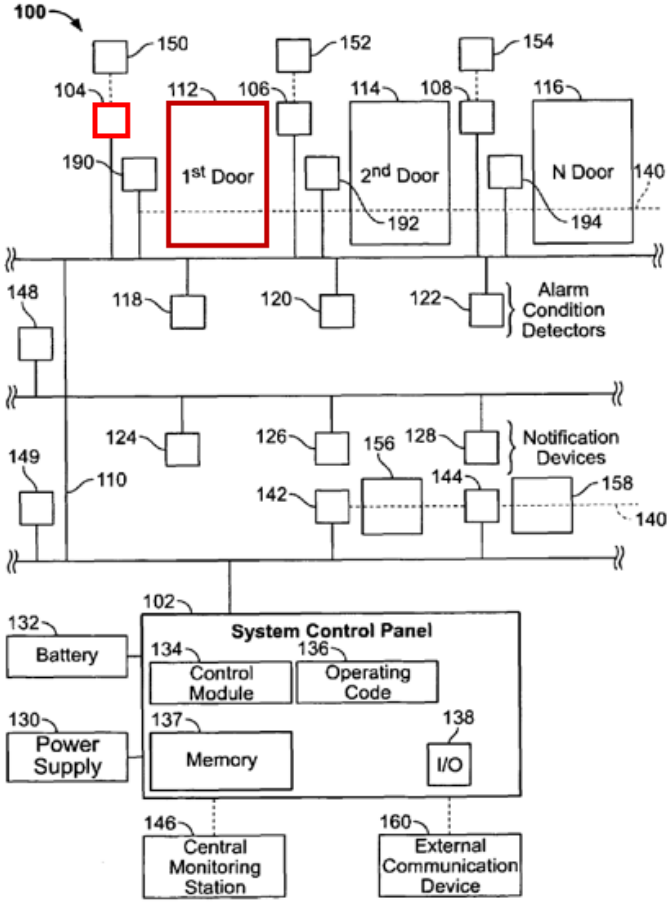

100
150
152
154
104
112
106
114
108
116
190
1st Door
2nd Door
N Door
140
192
194
148
118
120
122
Alarm Condition Detectors
124
126
156
128
Notification Devices
149
110
142
144
158
140
102
132
System Control Panel
Battery
134
136
Control Module
Operating Code
130
137
138
Power Supply
Memory
I/O
146
160
Central Monitoring Station
External Communication Device

FIG. 1

- **Fig. 2:**

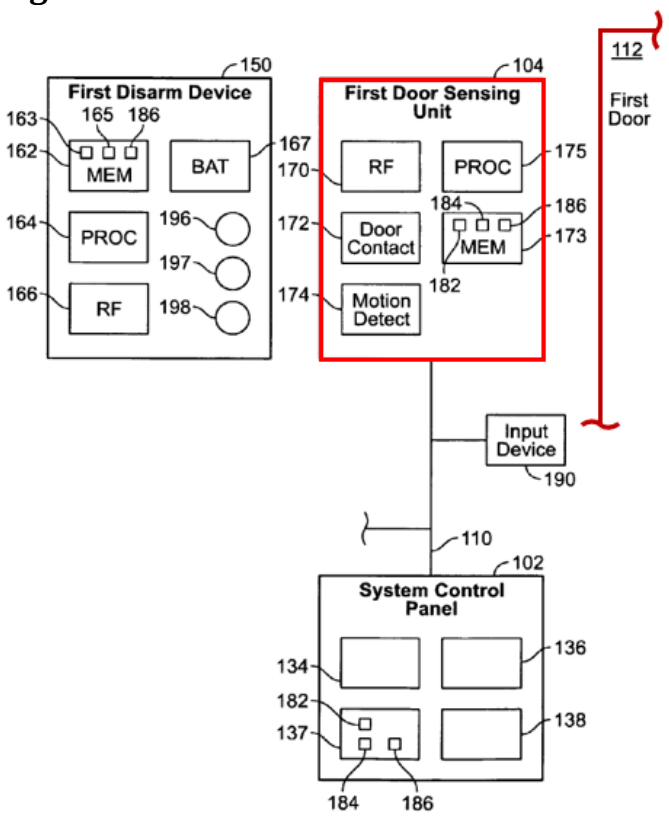


FIG. 2

- **3:1-5** ("The system 100 has one or more door sensing units, such as *first door sensing unit 104*, second door sensing unit 106 through N door sensing unit 108 which may be *configured to monitor first door 112*, second door 114, through N door 116, respectively.")
- **4:3-24** ("During normal operation, the security system 100 may be set in several modes, such as Armed Away Mode, Armed Stay Mode and Disarm Mode. Other modes of operation may be used.… *Armed Stay Mode arms the perimeter monitoring devices, such as the first through N door sensing units 104-108* and the first through N window sensors 142 and 144. *This mode will generate an alarm when any of the first through N doors 112-116 or first through N windows 156 and 158 are opened or otherwise compromised*, but allows people to move about within the perimeter 140 without generating an alarm.")
- ***See also* 2:60-67, 4:50-58.**

173. **Sharma** discloses a barrier alarm device in the form of a **door sensing unit 104** that is placed proximately to a **first door 112**. Sharma, 3:1-5. The **door**

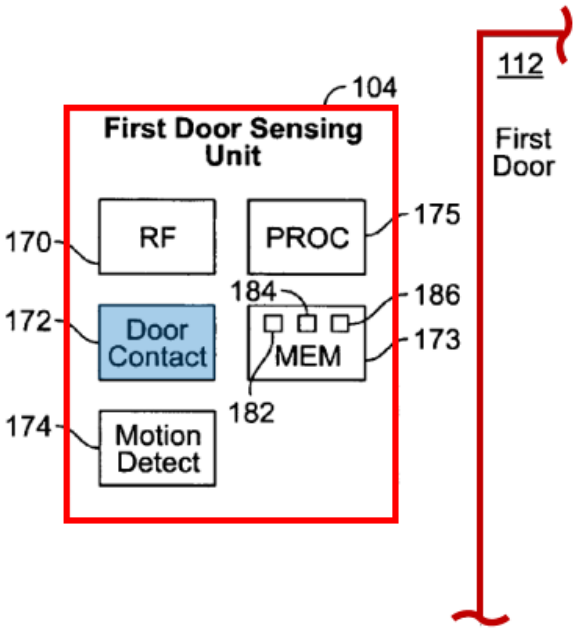
sensing unit 104 monitors the status of the **first door 112** and causes an alarm to be generated if the door is" opened or otherwise compromised." Sharma, 4:3-24.

(b) Element [1.a]

174. **Element [1.a] recites "a barrier status detection device for indicating that a barrier monitored by the barrier alarm device has been opened."** This element is met by Sharma.

175. **Sharma discloses a barrier status detection device for indicating that a barrier monitored by the barrier alarm device has been opened** (*e.g.*, "door sensing unit 104" includes "door contact 172" for generating a "door open signal" indicating that "first door 112" has been opened)**.** *See*, *e.g.*, Sharma (emphasis added):

- **Fig. 2 (excerpt):**



- **Fig. 5:**

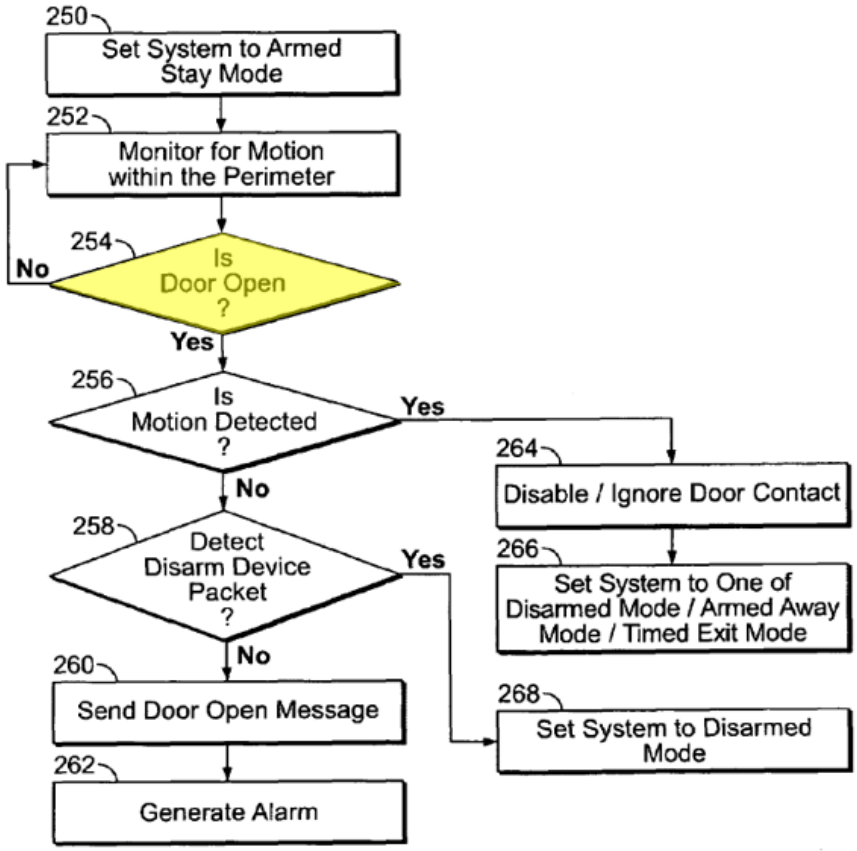


FIG. 5

- **4:50-53** ("*The first door sensing unit 104 has* an RF transceiver 170, *a door contact 172* and a motion detector 174. *The door contact 172* may be wireless and *may be used to detect whether the first door 112 is open* or closed.")
- **7:52-58** ("At 254, the processor 175 (FIG. 2) of the first door sensing unit 104 *determines whether the door contact 172 has detected that the first door 112 is open*. If the first door 112 is not open, the method returns to 252, monitoring for both motion and an open door. *If the first door 112 is open*, at 256 the processor 175 determines whether the motion detector 174 has detected motion within the perimeter 140.")
- **8:1-4** ("Returning to 256, if motion is detected, the method passes to 264 where the processor 175 may disable the door contact 172 and/or ignore the *door open signal from the door contact 172*.")
- ***See also* 6:6-7, 9:8.**

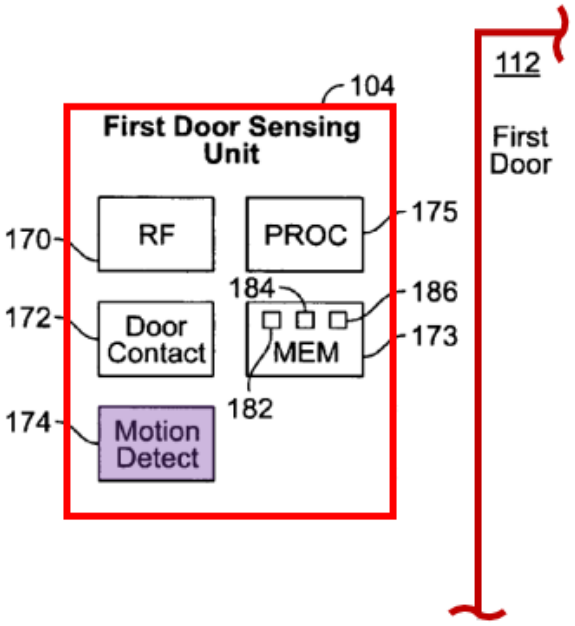
176. **Sharma** discloses that **door sensing unit 104** monitors and detects whether **first door 112** has been opened using its component **door contact 172**. Sharma, 4:50-53. The **door contact 172** produces signals when the **first door 112** has been opened that are read by the processor 175 for further action. Sharma, 7:52-58, 8:1-4. Therefore, **door contact 172** is a barrier status detection device that meets this claim element.

(c) Element [1.b]

177. **Element [1.b] recites "a human detection device for indicating that a human being is inside a premises in proximity to the barrier."** This element is met by Sharma.

178. **Sharma discloses a human detection device for indicating that a human being is inside a premises in proximity to the barrier** (*e.g.*, "door sensing unit 104" includes "motion detector 174" for detecting the presence of a human proximate to the inside of "first door 112," inside a "perimeter 140")**.** *See*, *e.g.*, Sharma (emphasis added):

- **Fig. 2 (excerpt):**



- **Fig. 4**

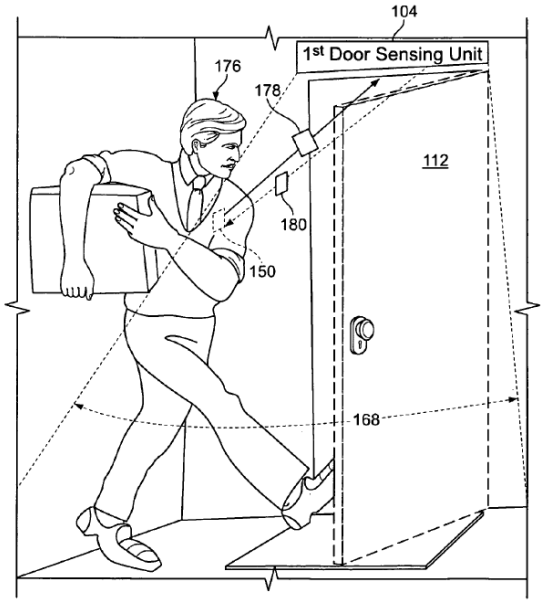


FIG. 4

- **Fig. 5**

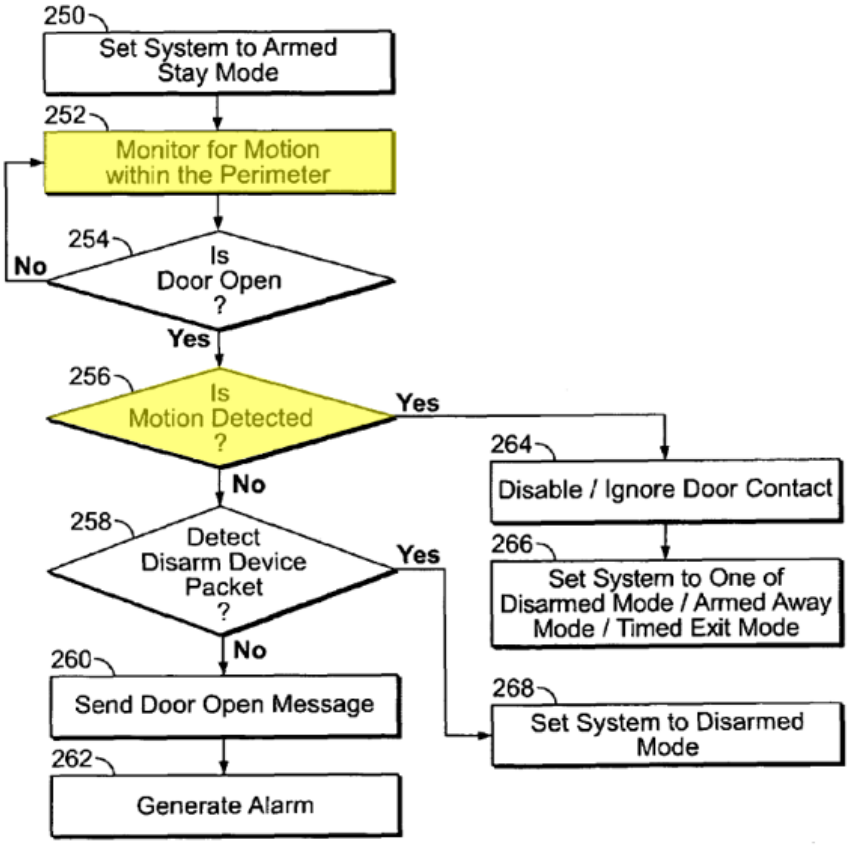


FIG. 5

- **4:50-56** ("*The first door sensing unit 104 has* an RF transceiver 170, a door contact 172 and *a motion detector 174*…. The motion detector 174 may be a passive infrared (IR) detector or other type of motion detector and may *sense motion proximate to the inside of the first door 112 (within the perimeter 140)*.")
- **7:47-51** ("At 252, *the motion detector 174 (FIG. 2) of the first door sensing unit 104 monitors the area within the perimeter 140 proximate to the inside of the first door 112 for motion*. Detection of motion by the motion detector 174 will not generate an alarm.")
- **7:56-8:4** ("If the first door 112 is open, at 256 *the processor 175 determines whether the motion detector 174 has detected motion within the perimeter 140*. If motion is not detected, the method passes to 258…. [¶] Returning to 256, *if motion is detected*, the method passes to 264 where the processor 175 may disable the door contact 172 and/or ignore the door open signal from the door contact 172.")
- ***See also* 9:5-7.**

179. **Sharma** discloses that its **door sensing unit 104** also includes a **motion detector 174** component that is used to monitor and detect motion that occurs proximate to the inside of the **first door 112**; Sharma provides defines proximate as the area within a perimeter 140 around the **first door 112**. Sharma, 4:50-56; 7:47-51. Processor 175 retrieves and uses the sensed data and resulting determinations about the presence of motion proximate to the **first door 112** from **motion detector 174** to make determinations about how to proceed with respect to the detected conditions. A person having ordinary skill in the art would have recognized that **motion detector 174** is a human detection device because Sharma teaches that **motion detector 174** may be implemented as "a passive infrared (IR) detector," and a person having ordinary skill would have understood that this necessarily detects humans because human beings emit infrared radiation. In fact, the '340 patent also describes implementing its human detection device using "an infrared transmitted/receiver." '340, 9:3-12. Moreover, Figure 4 in Sharma shows a human being whose presence is detected by motion detector 174 once they "move into the RF detection field 168." Sharma, Fig. 4, 5:62-6:1.

(d) Element [1.c]

180. **Element [1.c] recites "a transmitter for transmitting a timed alarm signal to a receiver associated with a security panel, the timed alarm signal for**

initiating a timer associated with the security panel." This element is met by Sharma.

181. **Sharma discloses a transmitter for transmitting a timed alarm signal to a receiver associated with a security panel** (*e.g.*, **processor 175** transmits signals to a receiver of "system control panel 102," over network 110, to enter a "Timed Exit Mode")**, the timed alarm signal for initiating a timer associated with the security panel** (*e.g.*, for initiating a 30 second timer before the system is rearmed)**.** *See*, *e.g.*, Sharma (emphasis added):

- **Fig. 2 (excerpt):**

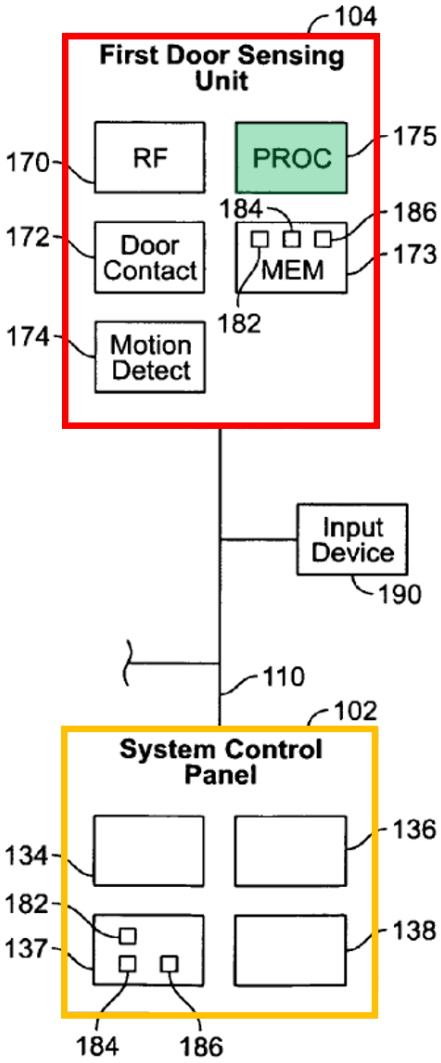


FIG. 2

- **Fig. 5:**

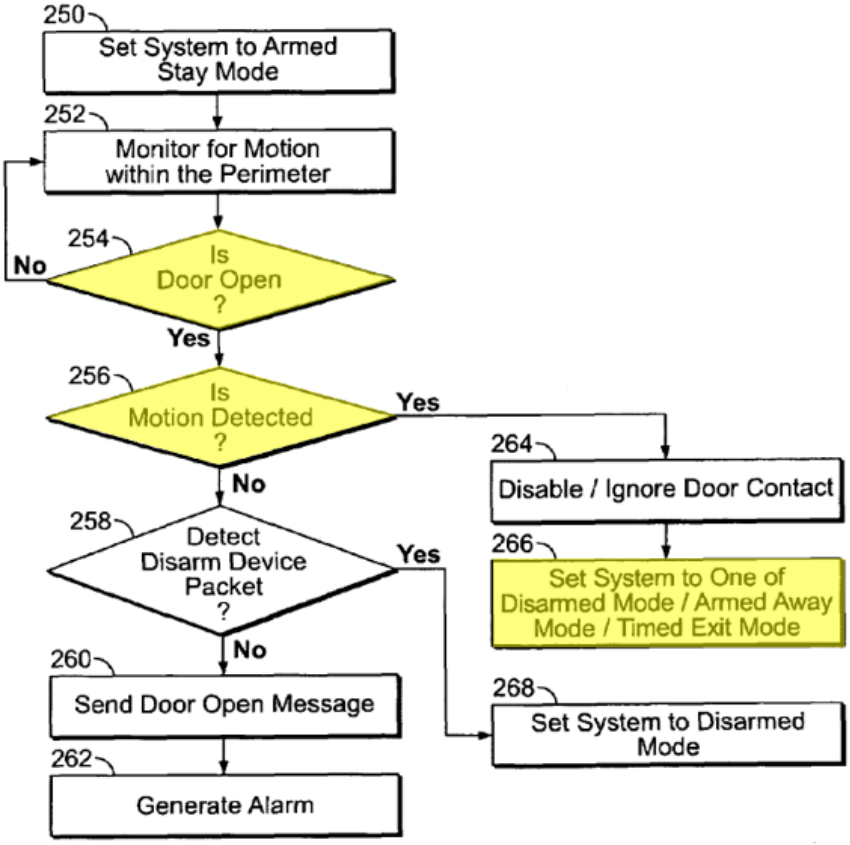


FIG. 5

- **1:54-57** ("A door sensing unit comprises *a first radio frequency (RF) transceiver interconnected with the system control panel* over a network.")
- **3:9-12** ("The first through N *sensing units 104*-108 *communicate with the system control panel 102 over the network 110*. Each of the door sensing units 104, 106, and 108 has a unique address on the network 110.")
- **3:45-48** ("Other *functions of the system control panel 102 may include displaying the status of the system 100, resetting a component, a portion, or all of the system 100*, silencing signals, turning off strobe lights, and the like.")
- **4:50** ("The first door sensing unit 104 has *an RF transceiver 170*….")
- **7:38-42** ("At 250, t*he system 100 is set to Armed Stay Mode*. The *system control panel 102 may send an activation message to each of the perimeter monitoring devices*, such as the first through Ndoor sensing units 104-108 and the first through N window sensors 142 and 144.")
- **8:6-21** ("At 266, *the processor 175 may send a signal to the system control panel 102 to set the system* 100 to Disarmed Mode. Therefore, if the person who exited the facility through the first door 112 returns and does not have a

disarm device, a false alarm will not be generated. Alternatively, the system 100 may be set to Armed Away Mode. *Alternatively, the system 100 may enter a Timed Exit Mode for a predetermined amount of time, such as 30 seconds.* When in Timed Exit Mode, the processor 175 may ignore the door control signal and/or disable the door contact 172. *After the predetermined amount of time has elapsed, the system 100 is reset to the Armed Stay Mode, continuing to provide protection from intruders.* Therefore, if the first door 112 is subsequently opened externally, an alarm is generated. The Timed Exit Mode allows people to leave the house or facility without having to interact with the system 100.")

- ***See also* Abstract.**

182. **Sharma** discloses that **door sensing unit 104** includes a **processor 175** that communicates and is interconnected with **system control panel 102** over network 110. On network 110, **door sensing unit 104** has a unique address on network 110. A person having ordinary skill in the art would have recognized or found obvious that the disclosed communications over the network 110 would necessarily include the use of components such as transmitters, receivers, and/or transceivers at the sending and receiving ends of the communications (for example, such transmission and receiving components must be used at **door sensing unit 104** and at **system control panel 102**) to facilitate the sending and receiving of the disclosed signals across the network.

183. **Sharma** further discloses that **system control panel 102** arms, disarms, and sets the mode of the system 100 based on signals transmitted to it by **processor 175**. Sharma, 1:64-67, 6:66-7:1, 7:61-64, 8:6-11. In one example, Sharma discloses that the system 100 enters a "Timed Exit Mode" after receiving a signal prompting

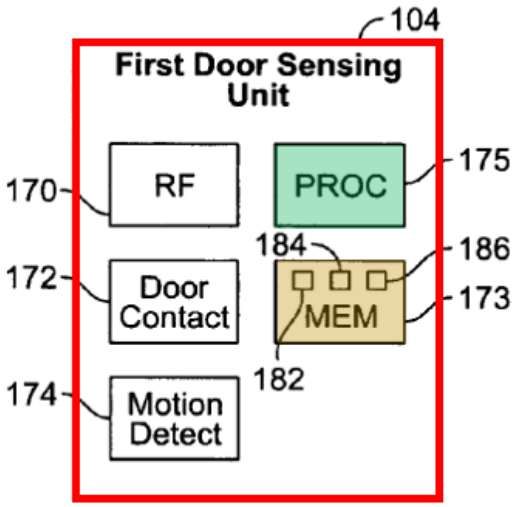
this state change. Sharma, 8:6-13. A person having ordinary skill in the art would have known that this signal to enter the Timed Exit Mode is a "timed alarm signal" because the signal is an alarm generated in response to detecting a possibly problematic condition (a door open and motion within perimeter 140 (in steps 254 and 256)) and the signal is sent to initialize a timer that runs for a predetermined amount of time (for example, 30 seconds); once the timer runs out, the system 100 (including **system control panel 102**) resets. Sharma, 8:6-21. Resetting the system, activating devices, and other responses to an elapsed timer that are disclosed by Sharma are functions directed by the **system control panel 102** (*see* Sharma, 3:45-48, 7:38-42), and therefore the timer that directs a system reset upon expiration is associated with **system control panel 102**.

(e) Element [1.d]

184. **Element [1.d] recites "a memory having processor-executable instructions stored thereon."** This element is met by Sharma.

185. **Sharma discloses a memory** (*e.g.*, "memory 173") **having processor-executable instructions stored thereon.** *See, e.g.*, Sharma (emphasis added):

- **Fig. 2 (excerpt):**



- **2:44-56** ("To the extent that the figures illustrate diagrams of the functional blocks of various embodiments, the functional blocks are not necessarily indicative of the division between hardware circuitry. Thus, for example, one or more of the functional blocks (e.g., *processors or memories*) may be implemented in a single piece of hardware (e.g., *a general purpose signal processor* or *a block or random access memory, hard disk, or the like*). Similarly, the programs may be stand alone programs, may be incorporated as subroutines in an operating system, may be functions in an installed software package, and the like. It should be understood that the various embodiments are not limited to the arrangements and instrumentality shown in the drawings.")
- **4:57-61** ("The system control panel 102 has *a control module 134 which provides control software and hardware to operate the system 100*. *Operating code 136 may be provided on a hard disk, ROM, flash memory, stored and run on a CPU card, or other memory*.")
- **4:56-58** ("A *memory 173* and a processor 175 *may also be within the first door sensing unit 104*")
- ***See also* 5:4-8, 6:46-56.**

186. **Sharma** discloses that its **door sensing unit 104** includes **processor 175** and **memory 173** components that may be implemented as a general purpose processor and RAM, hard disks, and other similar components. Sharma, 2:44-56, 4:56-57. A person having ordinary skill in the art would have recognized or found

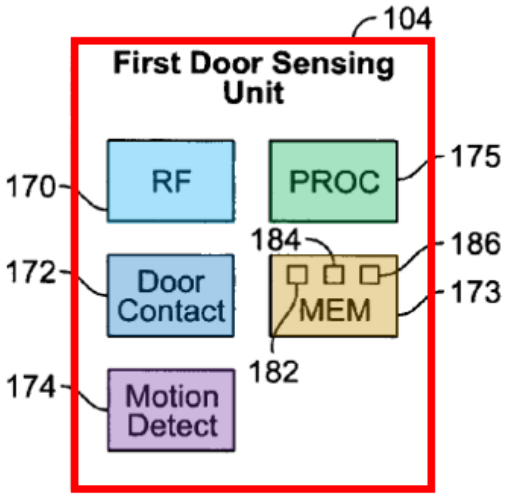
obvious that the **door sensing unit 104** would need to have stored executable instructions in **memory 173** for execution by the general purpose processor in order to perform the specific functions described by **Sharma**. For example, Sharma provides that **system control panel 102** includes a control module that operates based on "[o]perating code 136" that is "stored and run on … memory." Sharma 3:57-61.

(f) Element [1.e]

187. **Element [1.e] recites "a processor coupled to the barrier status detection device, the human detection device, the transmitter, and the memory, for executing the processor-executable instructions that cause the barrier alarm device to."** This element is met by Sharma.

188. **Sharma discloses discloses a processor** (*e.g.*, "processor 175") **coupled to the barrier status detection device** (*e.g.*, "door contact 172")**, the human detection device** (*e.g.*, "motion sensor 174")**, the transmitter** (*e.g.*, "RF transceiver 170")**, and the memory** (*e.g.*, "memory 173")**, for executing the processor-executable instructions** (*see* [1.d])**.** *See, e.g.*, Sharma (emphasis added):

- **Fig. 2 (excerpt):**



- **4:56-58** ("A memory 173 and *a processor 175 may also be within the first door sensing unit 104*")
- **6:47-50** ("…*processor 175 compares* the System ID 186 and the Device ID 163 sent in the disarm device packet 178 *to the values* (such as the System ID 186 and the list of approved Device IDs 182) *stored in the memory 173*.")
- **7:52-64** ("At 254, the *processor 175* (FIG. 2) of the first door sensing unit 104 *determines whether the door contact 172 has detected* that the first door 112 is open…. If the first door 112 is open, at 256 the *processor 175 determines whether the motion detector 174 has detected* motion within the perimeter 140. If motion is not detected, the method passes to 258 where the *processor 175 determines whether a valid disarm device packet 178 has been received by the RF transceiver 170*. If a valid disarm device packet 178 has not been received, the method passes to 260 where the *processor 175 sends a Door Open message to the system control panel 102*.")
- **8:1-4** ("…processor 175 may disable the door contact 172…")
- ***See also* 8:13-15, 8:27-29.**

189. **Sharma** discloses that the **barrier alarm device** includes **processor 300** that is coupled to other components of the **barrier alarm device** including the **barrier status detection device 306**, the **human detection device 304**, the **transmitter 308**, and the **memory 302**. Sharma provides that the processor executes the processor-executable instructions stored in the **barrier alarm device's memory**

to control the operations of the **barrier alarm device** in response to data from the other components to which **processor 300** is coupled.

(g) Element [1.f]

190. **Element [1.f] recites "respond to the barrier status detection device indicating that the barrier has been opened by determining whether the human detection device indicates that the human being is inside the premises in proximity to the barrier."** This claim is met by Sharma.

191. **Sharma discloses the processor executing the processor-executable instructions to cause the barrier alarm device to** (*e.g.*, *see* [1.e]) **respond to the barrier status detection device indicating that the barrier has been opened** (e.g., responds to "door contact 172" indicating that "first door 112" has been opened) **by determining whether the human detection device indicates that the human being is inside the premises in proximity to the barrier** (*e.g.*, responds by determining whether "motion detector 174" detects motion indicative of a human within perimeter 140 proximate to first door 112; *see also* [1.b])**.** *See*, *e.g.*, Sharma (emphasis added):

- **Fig. 5:**

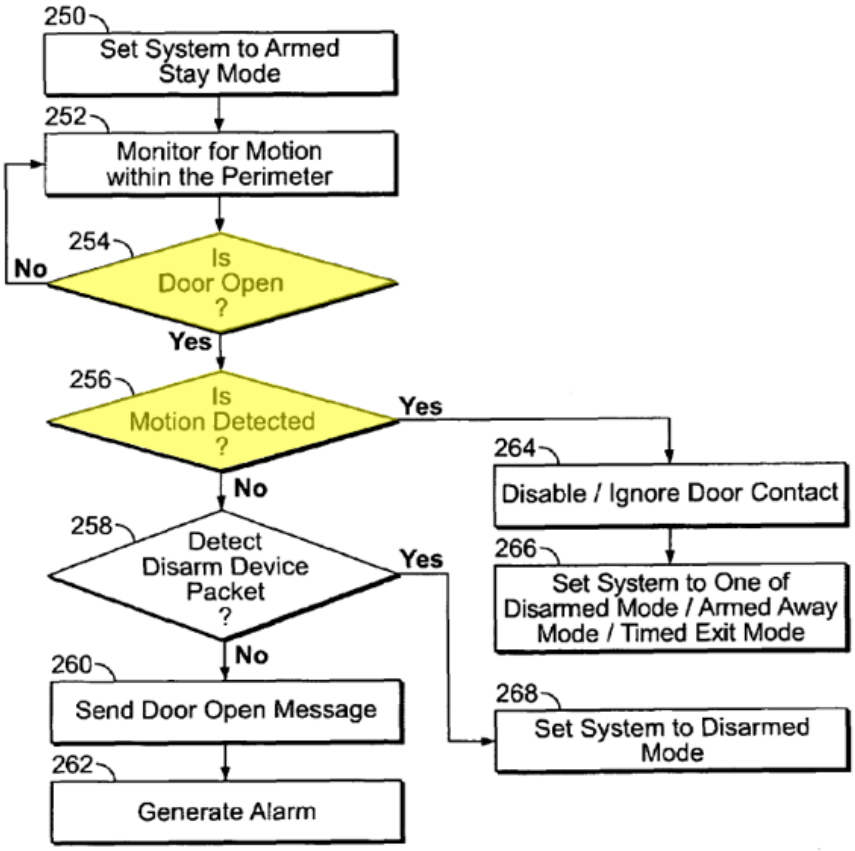


FIG. 5

- **4:50-56** ("The motion detector 174 may be a passive infrared (IR) detector or other type of motion detector and may *sense motion proximate to the inside of the first door 112 (within the perimeter 140)*.")
- **7:52-8:2** ("At 254, the processor 175 (FIG. 2) of the first door sensing unit 104 determines whether the door contact 172 has detected that the first door 112 is open. If the first door 112 is not open, the method returns to 252, monitoring for both motion and an open door. *If the first door 112 is open, at 256 the processor 175 determines whether the motion detector 174 has detected motion within the perimeter 140. If motion is not detected*, the method passes to 258…. [¶] Returning to 256, *if motion is detected*, the method passes to 264….")

192. **Sharma** discloses that **door sensing unit 104's processor 175** "determines whether the **door contact 172** has detected that the **first door 112** is open," and if it determines that **first door 112** is in fact open, the **processor 175** then

responds by next "determin[ing] whether the **motion detector 174** has detected movement" inside the premises corresponding to **first door 112**. Sharma, 7:52-58. As I discussed for element [1.b], **motion detector 174** is positioned such that it can monitor the portion of the premises that is "proximate to the inside of **first door 112**" and accordingly detects the motion of humans within this area. Sharma, 7:46-51; *see* [1.b].

(h) Element [1.g]

193. **Element [1.g] recites "transmit, via the transmitter, the timed alarm signal to the receiver only when it is determined that the human detection device indicates that the human being is inside the premises in proximity to the barrier."** This claim is met by Sharma.

194. **Sharma discloses the processor executing the processor-executable instructions to cause the barrier alarm device to** (*e.g.*, *see* [1.e]) **transmit, via the transmitter, the timed alarm signal to the receiver** (*e.g.*, transmit to the system control panel 102, via "RF transceiver 170," the signal to enter the "Timed Exit Mode," which initiates a 30 second timer before the system is rearmed; *see* [1.c]) **only when it is determined that the human detection device indicates that the human being is inside the premises in proximity to the barrier** (*e.g.*, only when "motion is detected" by "motion detector 174")**.** *See*, *e.g.*, Sharma (emphasis added):

- **Fig. 5:**

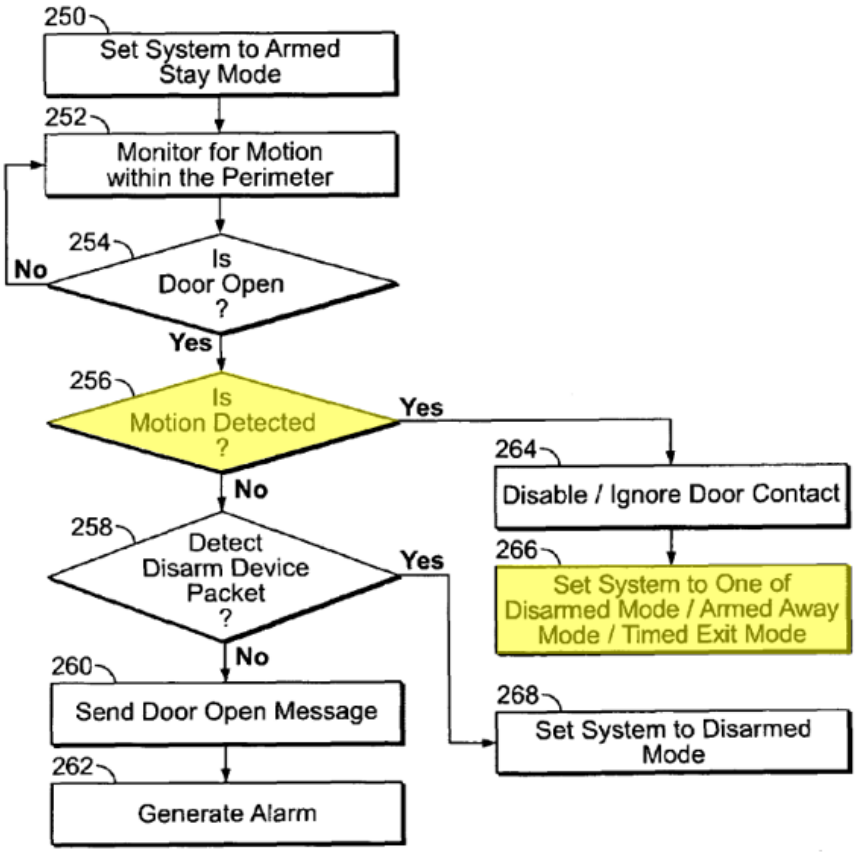


FIG. 5

- **1:54-57** ("A door sensing unit comprises *a first radio frequency (RF) transceiver interconnected with the system control panel* over a network.")
- **7:52-8:21** ("If the first door 112 is open, *at 256 the processor 175 determines whether the motion detector 174 has detected motion within the perimeter 140.*… [¶] Returning to 256, *if motion is detected*, the method passes to 264 where the processor 175 may disable the door contact 172 and/or ignore the door open signal from the door contact 172…. [¶] At 266, *the processor 175 may send a signal to the system control panel 102 to set the system* 100 to Disarmed Mode…. *Alternatively, the system 100 may enter a Timed Exit Mode for a predetermined amount of time, such as 30 seconds.* When in Timed Exit Mode, the processor 175 may ignore the door control signal and/or disable the door contact 172. *After the predetermined amount of time has elapsed, the system 100 is reset to the Armed Stay Mode, continuing to provide protection from intruders.* Therefore, if the first door 112 is subsequently opened externally, an alarm is generated. The Timed Exit Mode allows people to leave the house or facility without having to interact with the system 100.")

195. *See* my discussion for elements [1.c]-[1.f]. As I discussed for element [1.c], **Sharma** discloses that **door sensing unit 104** includes the **processor 175** and **RF transceiver 170** components, and **Sharma** also discloses that **processor 175** is configured to send a timed alarm signal to **system control panel 102** that directs system 100 to enter a "Timed Exit Mode" upon the identification of particular circumstances. Specifically, **Sharma** discloses that **processor 175** only transmits a signal that directs the system 100 to enter the Timed Exit Mode when "motion detector 174" detects motion indicative of a human being present within the perimeter 140 that defines a space proximate to first door 112; for example, in Figure 5, Sharma provides that detecting motion at Step 256 is a prerequisite for later setting the system to one of several modes, among which "Timed Exit Mode" is included. Sharma, Fig. 5.

(i) Element [11.pre]

196. **Element [11.pre] recites "A method, comprising."** This element is met by Sharma.

197. **Sharma discloses a method** (*e.g.*, a "method"). *See*, *e.g.*, Sharma (emphasis added):

- **5:55-56** ("… *a method for disarming the security system 100* using one of the disarm devices 150-154.")
- **7:26-28** ("… *a method for preventing the door sensing units from generating a false alarm* when the security system 100 is in the Armed Stay Mode.")

198. **Sharma** explicitly discloses several methods related to the functioning of security systems.

(j) Element [11.a]

199. **Element [11.a] recites "in response to a barrier status detection device associated with a barrier alarm device indicating that a barrier being monitored by the barrier alarm device has been opened, determining whether a human detection device associated with the barrier alarm device indicates that a human being is inside a premises monitored by a central security panel in proximity to the barrier."** This claim is met by Sharma.

200. **Sharma discloses in response to a barrier status detection device associated with a barrier alarm device indicating that a barrier being monitored by the barrier alarm device has been opened** (e.g., responds to "door contact 172" indicating that "first door 112" has been opened)**, determining whether a human detection device associated with the barrier alarm device indicates that a human being is inside a premises monitored by a central security panel in proximity to the barrier** (*e.g.*, responds by determining whether "motion detector 174" detects motion indicative of a human within perimeter 140 proximate to first door 112; *see also* [1.b])**.** *See*, *e.g.*, Sharma (emphasis added):

- **Fig. 5:**

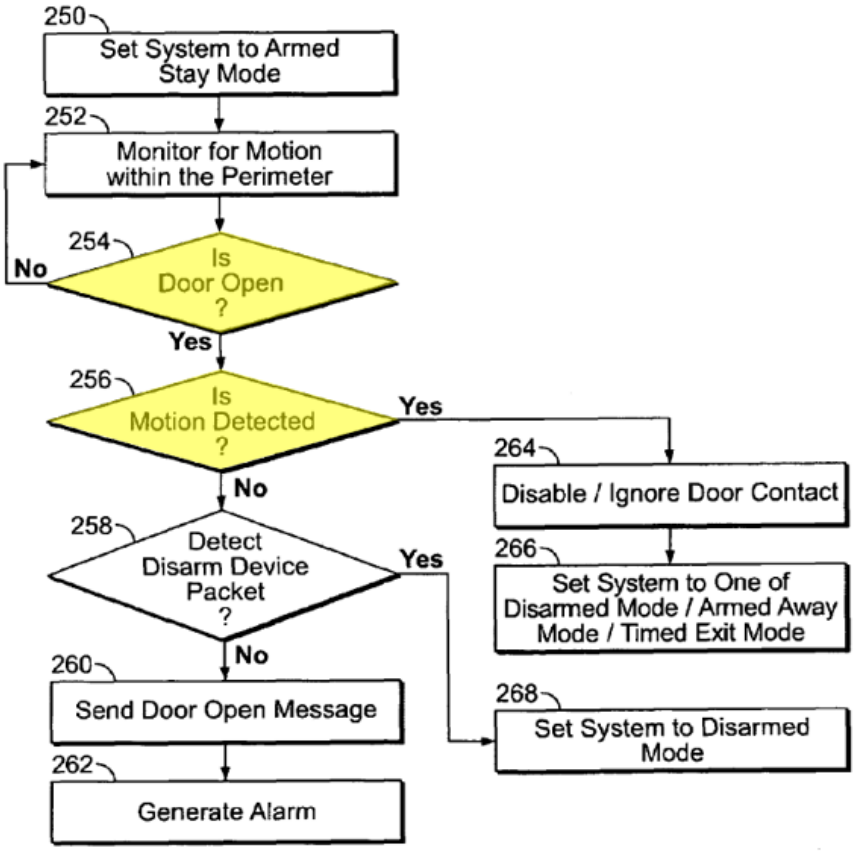


FIG. 5

- **4:50-56** ("The motion detector 174 may be a passive infrared (IR) detector or other type of motion detector and may *sense motion proximate to the inside of the first door 112 (within the perimeter 140)*.")
- **7:52-8:2** ("At 254, the processor 175 (FIG. 2) of the first door sensing unit 104 determines whether the door contact 172 has detected that the first door 112 is open. If the first door 112 is not open, the method returns to 252, monitoring for both motion and an open door. *If the first door 112 is open, at 256 the processor 175 determines whether the motion detector 174 has detected motion within the perimeter 140. If motion is not detected*, the method passes to 258…. [¶] Returning to 256, *if motion is detected*, the method passes to 264….")

201. **Sharma's** barrier alarm device of claim 1, which also transmits alarm signals to, and is therefore monitored by, a central security panel, is configured to perform a method including the same steps claimed in [11.a]. *See* [1.c]-[1.f].

Sharma therefore renders obvious [11.a] for the same reasons discussed in [1.f]. In particular, **Sharma** discloses that **door sensing unit 104's processor 175** "determines whether the **door contact 172** has detected that the **first door 112** is open," and if it determines that the **first door 112** is in fact open, the **processor 175** then responds by next "determin[ing] whether the **motion detector 174** has detected movement" inside the premises indicative of a person present close to the **first door 112**. Sharma, 7:52-58. As I discussed for element [1.b], **motion detector 174** monitors the premises "proximate to the inside of **first door 112**" and detects the motion of humans, and therefore is used to determine that there is a human being inside the monitored premises. Sharma, 7:46-51; *see* [1.b].

(k) Element [11.b]

202. **Element [11.b] recites "transmitting by the barrier alarm device a timed alarm signal to the central security panel for the purpose of initiating a timer associated with the central security panel only when it is determined that the human detection device indicates that the human being is in inside the premises and in proximity to the barrier."** This claim is met by Sharma.

203. **Sharma discloses transmitting by the barrier alarm device a timed alarm signal to the central security panel for the purpose of initiating a timer associated with the central security panel** (*e.g.*, transmit to the system control panel 102, via "RF transceiver 170," the signal to enter the "Timed Exit Mode,"

which initiates a 30 second timer before the system is rearmed; *see* [1.c]) **only when it is determined that the human detection device indicates that the human being is in inside the premises and in proximity to the barrier** (*e.g.*, only when "motion is detected" by "motion detector 174")**.** *See, e.g.*, Sharma (emphasis added):

- **Fig. 5:**

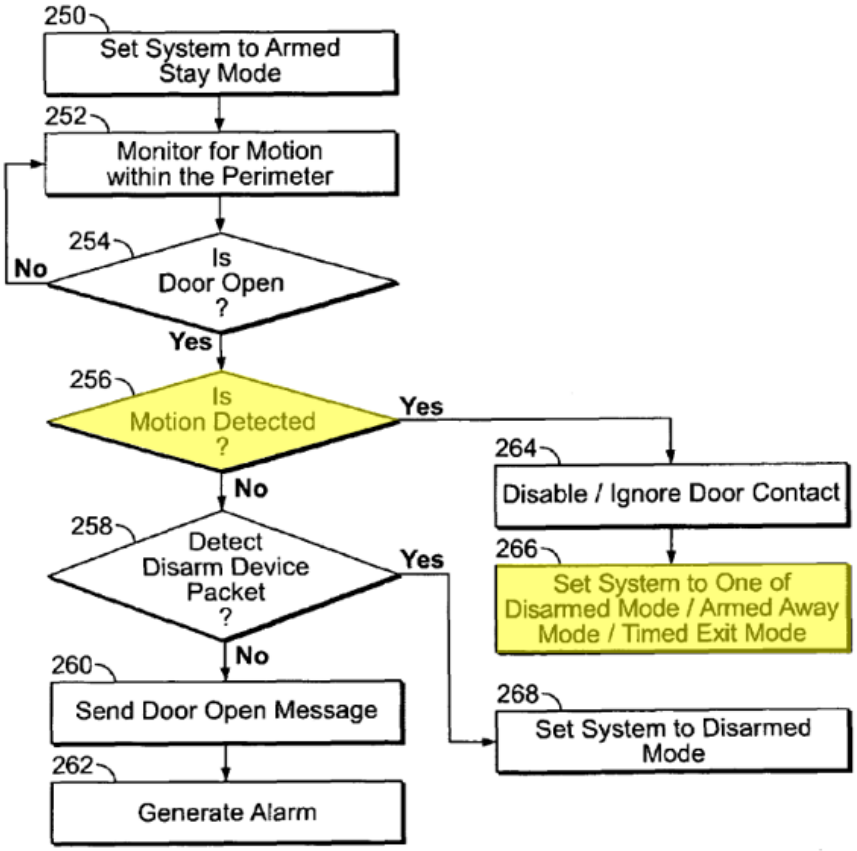


FIG. 5

- **7:52-8:21** ("If the first door 112 is open, *at 256 the processor 175 determines whether the motion detector 174 has detected motion within the perimeter 140.*… [¶] Returning to 256, *if motion is detected*, the method passes to 264 where the processor 175 may disable the door contact 172 and/or ignore the door open signal from the door contact 172…. [¶] At 266, *the processor 175 may send a signal to the system control panel 102 to set the system* 100 to Disarmed Mode…. *Alternatively, the system 100 may enter a Timed Exit Mode for a predetermined amount of time, such as 30*

seconds. When in Timed Exit Mode, the processor 175 may ignore the door control signal and/or disable the door contact 172. *After the predetermined amount of time has elapsed, the system 100 is reset to the Armed Stay Mode, continuing to provide protection from intruders.* Therefore, if the first door 112 is subsequently opened externally, an alarm is generated. The Timed Exit Mode allows people to leave the house or facility without having to interact with the system 100.")

204. *See* my discussion for elements [1.c]-[1.g]. **Sharma** discloses that **door sensing unit 104** includes **processor 175** and **RF transceiver 170** components, and that the **processor 175** is programmed to send to **system control panel 102** a timed alarm signal that directs system 100 to enter a "Timed Exit Mode." **Sharma** discloses that **processor 175** only transmits a signal to enter the Timed Exit Mode when "motion detector 174" detects motion that indicates the presence of a human within perimeter 140 that is proximate to first door 112.

VIII. SECONDARY CONSIDERATIONS

205. I have not seen any evidence in the prosecution history of the '340 patent or any related application that I considered of any arguments regarding secondary considerations exist. Nor have I seen any evidence that any such evidence would have a nexus to any of the Challenged Claims 1-2, 6, 11-12, and 16. Moreover, as shown above with respect to the prior art referenced in Section VII, any alleged solutions to problems or unexpected results in the '340 patent were already well known.

IX. CONCLUSION

206. In summary, I have concluded that the Challenged Claims 1-2, 6, 11-12, and 16 are rendered obvious over the prior art references as discussed above. Specifically, in my opinion, for at least the reasons above, Challenged Claims 1-2, 6, 11-12, and 16 of the ’340 patent are rendered obvious as follows:

Ground	**’340 Patent Claims**	**Prior Art References**
1	1-2, 6, 11-12, 16	Lamb in view of Williams
2	1, 11	Sharma

207. To the extent it is argued that any further disclosure is required for an element in the Challenged Claims 1-2, 6, 11-12, and 16 that I have identified as being disclosed, a person having ordinary skill in the art would certainly have found that element obvious to include based on the same explicit disclosure or inherent disclosures and analysis I have identified above.

208. I reserve the right to supplement my opinions in the future to respond to any arguments that Patent Owner or its expert(s) may raise and to take into account new information as it becomes available to me.

209. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

210. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed this March 29, 2023, in Holmdel, NJ.

Respectfully submitted,



Bruce McNair

APPENDIX A

(C*urriculum Vitae*)

Bruce McNair

1 Iron Hill Drive
Holmdel, NJ 07733
bmcnair@novidesic.com
1-732-264-5244

Career Summary

- Sixty years engineering research, design, development, systems engineering experience in communications systems (including extensive background in wireless communications and system/network security)
- Twenty four years as a well-rated member of one of world's most highly respected R&D organizations, recognized for breadth, depth and practicality of expertise
- Extensive experience teaching technical short courses for premiere educational programs over a fourteen year period
- Full time university educator for fifteen years with experience teaching a broad set of courses focusing on practical engineering approach
- On-line university educator for twenty years teaching well-attended graduate courses in wireless and security technologies

Research interests

- High speed wireless data networking
- System/network security
- Geolocation technology
- Real-time digital signal processing
- Software-Defined Radio technology
- Broadband Powerline (BPL) technology

Present Organizations

- Stevens Institute of Technology,
- Novidesic Communications, LLC

Job Titles

- Distinguished Service Professor of Electrical and Computer Engineering
- Founder, Chief Technology Officer

Education

- M.E., E.E., Stevens Institute of Technology, 1974
- B.E. (with Honor), Stevens Institute of Technology, 1971
- Completed qualifiers and course work for PhD in Computer Science at Stevens

Relevant Experience

January 2003 – present – on-line teaching professor – Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ;
Teach several well-enrolled on-line graduate courses in wireless security, information systems security and physical design of wireless communications systems.

August 2002 – December 2017 (retired) – Distinguished Service Professor of Electrical and Computer Engineering, Program Director, Computer Engineering graduate program, Stevens Institute of Technology, Hoboken, NJ;
Design and manage the Senior Design Project, a two-semester program that forms a substantial portion of the senior year in the engineering program. This project comprises a large fraction of the seniors' efforts and serves to provide real-world engineering design experiences for the student. Teach a large number of well-enrolled graduate and undergraduate core and elective courses. Conduct research in wireless systems, geolocation services, and broadband powerline (BPL) systems, particularly security needs and solutions. Member of Stevens Intellectual Property Review Board, Stevens Honor Board Advisory Council, Stevens' Schaeffer School of Engineering and Science Promotion and Tenure Committee, and the Senior Design Coordinator Committee.

February 2002 – present – CTO, Novidesic Communications, LLC, Holmdel, NJ;
Founded a technical consulting company, providing expert witness support and testimony, telecommunications, wireless networking, security, software, computing, product evaluation, proof-of-concept prototyping, and web site design guidance to individuals and small businesses. Clients include health care facilities, patent attorneys, major telecommunications providers, venture capitalists, major component manufacturing company, start-up hardware and concept development companies. Supported technology needs of small local business leading to Phase I and Phase II SBIR funding in the area of RFID with patented technology. Provide IP portfolio evaluation. Expert witness in patent litigation with experience testifying at deposition and trial as well as preparing USPTO IPR declarations.

August 2011 – February 2012 – Part-time consultant, Lockheed-Martin, Moorestown, NJ;
Support development of advanced radar systems and interactions with other wireless systems.

2010 – 2015 (part-time, on an as-needed basis) – Senior Systems Engineer consultant, AT&T Government Solutions, Columbia, MD;
Support AT&T's projects with the US Government customers on defense and intelligence-related systems, drawing on previous knowledge and experience in signal processing, wireless systems, telephone and computer networks, and secure system design.

Relevant Experience (continued)

May 1994 to February 2002 (retired) -- Wireless Systems Research Department, AT&T Bell Labs/ AT&T Labs - Research, Holmdel/Red Bank/Middletown, NJ
Member of Technical Staff/Research Staff Member/Principal Technical Staff Member/Technology Consultant; Investigating high-speed, high-mobility wireless data communications systems for untethered access to high speed global networks. Proposed and investigated IEEE 802.11(a & b) physical and MAC layer extensions to outdoor, high mobility environment. Efforts involved system architecture, system control, real-time DSP programming in C, high-speed hardware design, RF design, analog, RF interfacing, Matlab/SIMULINK simulation and experimental investigations. Responsible for complete design, implementation and characterization of a multiple TMS320C40-based 384 kb/s OFDM transmission system and definition/design of advanced signal processing platforms. Recent research extended results to 5-40 Mb/s with TMS320C62/FPGA-based platform and incorporated 802.11a and DVB-T technology. Previous research involved speech quality/data rate enhancements to IS-136, the North American TDMA cellular standard.

November 1987 to April 1994 -- Security and System Reliability Architecture Group, AT&T Bell Labs, Holmdel, NJ
Technical Manager; Created, staffed, and led a group of security, systems reliability and fraud control experts to assess security/quality of products, services, operations systems, communications networks, operating systems, and work centers and to recommend, specify, and prototype cost effective improvements. Created corporate process to build security into the development process. Transformed small (2 person) corporate-funded activity into well-staffed (multi million dollar), successful business unit supported program. Served as security technologies subject matter expert for AT&T Corporate Security and other (AT&T and outside) organizations

May 1982 to October 1987 -- various AT&T Bell Labs organizations, MTS - Supervisor; System Design, Exploratory Development, Applied Research, and Final Product Development of secure voice terminals, modems, speech recognition and speaker verification systems, security chips, encryption devices, and network management systems

June 1978 to April 1982 -- various AT&T Bell Labs organizations, Member of Technical Staff, System design, digital hardware design and simulation of wide area (X.25) data communications networks and high-speed data transmission techniques for voiceband modems. Led $1M IR&D secure voice terminal initiative, ultimately resulting in promotion to MTS-Supervisor and laying groundwork for AT&T's breakthrough success in NSA’s STU-3 program.

Relevant Experience (continued)

June 1971 to February 1973, January 1974 to June 1978 -- U.S Army Communications R&D Command, Fort Monmouth, NJ. GS-7, 9, 11 & 12 Electronic Engineer (GS-0855)
Development of tactical military radio communications equipment, specializing in modulation, data transmission, communications security and electronic warfare (frequency hopping and direct sequence spread spectrum) for the SINCGARS VHF-FM radio system.

March 1973 to December 1973 -- ITT Defense Communications Division, Nutley, NJ.
Junior Member of Technical Staff; Designed, developed and tested software and digital hardware for portable satellite terminals for use by White House and the world's first hardware implementation of a 2400 bps Linear Predictive Coder (LPC) secure speech transmission system.

Patents, Presentations and Publications

Twenty six U.S. patents and nineteen international patents granted (several pending) in areas such as data transmission, cryptographic techniques, speech processing, video processing, security systems, user authentication, fraud control, synchronization, dynamic channel assignment, localization techniques, hazardous voltage detection, RFID, biomedical applications, vibration energy harvesting, solar energy harvesting for portable devices, etc.

Presented numerous well-rated short courses in Digital Communications, Digital Telephony, Digital Signal Processing, and Wireless Communications, & Security. Course sponsors included: Bell Labs In-hours Continuing Education Program, George Washington University, University of Maryland, UCLA Extension, Johns Hopkins University – Organizational Effectiveness Institute, Berlin (Germany) Continuing Engineering Education Program, Monmouth University, and the Fort Monmouth Education Center.

Several papers presented at IEEE Vehicular Technology and other Conferences and published in AT&T Technical Journal, IEEE Transactions on Wireless Communications, and IEEE Communications Magazine on various topics in wireless systems and security.

Skills

System/network architecture, communications system design, digital hardware design, RF design, signal processing, real-time DSP programming, software design and coding, proof-of-concept prototyping, designing and conducting laboratory research experiments, OFDM, TDMA/IS-136, FPGA, encryption, computer network security, threat assessment, data communications protocols, computer architecture, digital and analog video systems, system & link-level simulation, UNIX/Linux, Windows, C/C++, Matlab/Simulink, MathCad, PASCAL, Algol, SNOBOL, Verilog, VHDL, FORTRAN. Recruitment, development and management of highly effective technical staff. Highly effective technical presentations and training sessions to any level audience. Well-developed technical writing skills. Preparation, deposition, and testifying regarding expert report for patent infringement/non-infringement/validity/invalidity and other litigation matters. Assist in claim construction and prior art research for patent litigation.

Other information

U.S Citizen. Held Top Secret - Sensitive Compartmented Information (TS/SCI) clearance with full scope polygraph until October 2015.

Selected as one of twenty-six finalists among 490 entrants in the 2014 Bell Labs Prize competition for proposal “High-precision, low-cost, low-power indoor geolocation techniques.”

Stevens Institute of Technology, Henry Morton Distinguished Teaching Professor, 2013-2014.

Named to New Jersey Inventors Hall of Fame, Inventor of the Year (2012) for “Patented/Innovative Research and Entrepreneurial Leadership Related to: Groundbreaking modem development and next generation wireless data communications systems”

Mentored two AT&T Labs Fellowship Program (ALFP) participants, three students in the MentorNet program, 5 Bell Labs Early Career Advisory Program (ECAP) participants, numerous summer students (graduate and undergraduate), several new employees, and all of the staff in groups I have managed.

Advised a significant fraction of ECE Senior Design groups, numerous graduate students; participation in thesis committees of several Stevens PhD students in various departments, including Physics, Computer Science, Mechanical Engineering, and ECE. Consult with non-ECE students on ECE aspects of their Senior Design projects

Mentor summer students at Stevens in NSF-funded Research Experience for Undergraduates (co-PI).

Stevens Institute of Technology, Schaefer School of Engineering, Undergraduate Teaching Award, December 2006.

Life Senior Member, Institute of Electrical and Electronic Engineers - Member of Communications, Signal Processing, Computer and Education Societies

Member, American Society for Engineering Education

Secretary, IEEE Communications Society Communications Security Committee

Identified by Rutberg & Co. Investment Bankers (San Francisco) as member of a group of 213 “Top Wireless Influencers: 2002”

Member of the Council of Communications Advisors

Amateur radio operator licensed since 1963, Amateur Extra Class since 1970

Contact Information

1 Iron Hill Drive
Holmdel, NJ 07733
(732) 264-5244
Cellular (732) 371-5026

bmcnair@novidesic.com
http://www.novidesic.com

US Patents

- “Liquid Crystal Display using the photovoltaic behavior of LED backlights as a source of electrical energy.” US Patent #10,310,326, June 4, 2019.
- “Method and apparatus for locating and distinguishing blood vessel.” US Patent #8,764,663, July 1, 2014.
- “Secure IP access protocol framework and supporting network architecture,” US Patent #8,046,577, October 25, 2011.
- “Method for Estimating Time and Frequency Offset in OFDM Systems,” US Patent #7,990,839, August 2, 2011.
- “Simulcasting OFDM system having mobile station location identification,” US Patent 7,962,162, June 14, 2011.
- “RFID Devices for Verification of Correctness, Reliability, Functionality and Security,” US Patent 7,712,674, May 11, 2010.
- ““Dynamic Channel Assignment,” US Patent 7,457,259, November 25, 2008.
- ““RFIDs Embedded into Semiconductors,” US Patent 7,348,887, March 25, 2008.
- “Method for Estimating Time and Frequency Offset in OFDM Systems,” US Patent #7,310,302, December 18, 2007.
- “Mobile Device Having Network Interface Selection,” US Patent #7,180,876, February 20, 2007.
- "Dynamic Channel Assignment," US Patent #6,954,465, October 11, 2005.
- “Method for Estimating Time and Frequency Offset in OFDM Systems,” US Patent #6,891,792, May 10, 2005.
- "Security System Providing Lockout for Invalid Access Attempts," US Patent #5,559,505, September 24, 1996.
- "Telecommunications Fraud Detection Scheme," US Patent #5,504,810, April 2, 1996.
- "Authenticator Card and System," US Patent #5,450,491, September 12, 1995.
- "Secure Telecommunications," US Patent #5,392,357, February 21, 1995.
- "Data Message Storage and Pickup Service,” US Patent #5,392,336, February 21, 1995.
- "System and Method for Granting Access to a Resource," US Patent #5,375,244, December 20, 1994.
- "Secure Teleconferencing," US Patent #5,353,351, October 4, 1994.
- "Method and Apparatus for Processor Based Encryption," US Patent #5,278,905, January 11, 1994.
- "Centralized Security Control System," US Patent # 5,276,444, January 4, 1994.
- "Technique for Voice Based Security System," US Patent #5,265,191, November 23, 1993.

US Patents (continued)

- "Video Scrambling System", US Patent # 5,206,906, April 27, 1993.
- "Cryptographic Transmission System," US Patent #4,642,424, February 10, 1987.
- "Processing of Encrypted Voice Signals," US Patent #4,608,455, August 26, 1986.
- "Control of Coefficient Drift for Fractionally Spaced Equalizers," US Patent #4,376,308, March 8, 1983

Several other published and unpublished US patents pending

International Patents

- “Voltage-controlled apparatus for battery-powered electronic devices,” EP Patent #0568237 B1, January 23, 2002.
- “A Dynamic Channel Assignment,” EP Patent #1,137,299, September 26, 2001.
- “Data Message Storage and Pickup Service,” EP Patent #0626776 B1, April 7, 1999.
- “Data Message Storage and Pickup,” Canadian Patent #CA-2119227A1, February 24, 1998.
- “Centralized Security Control System,” Canadian Patent #CA-2078077, January 27, 1998.
- “Improved centralized security control system and method,” EP Patent #0534679. August 12, 1997.
- “Authenticator Card with Changing Bar Code Pattern,” EP Patent #0,715,789, June 12, 1996.
- “Technique for voice-based security systems,” Canadian Patent #CA-2072172, April 30, 1996.
- “Method and apparatus for user identification and verification of data packets in a wireless communications network,” EP Patent #0,689,316, December 27, 1995.
- “Central Difference Control System,” Japanese Patent #1995-131526, May 19, 1995.
- “Authenticator Card with Changing Bar Code Pattern,” WO Patent #1995/006371, March 2, 1995.
- “Method for safety system of voice base and device therefore,” Japanese Patent #1995-049696, February 21, 1995.
- “Data message storage and pick up service, EP Patent #0,626,776, November 30, 1994.
- “Method for safety system of voice base and device therefore,” Japanese Patent #1995-049696, February 21, 1995.
- “Data message storage and pick up service, EP Patent #0,626,776, November 30, 1994.
- “Apparatus for battery type electronic device,” Japanese Patent #1994-138983, May 20, 1994.
- “Method and system for making communication via exchange network available, method for providing,” Japanese Patent #1994-085811, March 25, 1994.

International Patent (continued)

- Voltage-controlled apparatus for battery-powered electronic devices," EP Patent #0,568,237, November 3, 1993
- "Security node in switched telecommunication network", EP Patent #0,553,553, August 4,1993.
- "Improved centralized security control system and method," EP Patent 0,534,679, March 31, 1993.
- "An improved technique for voice-based security systems," EP Patent #0,533,396, March 24, 1993.
- "Cryptographic Transmission System," Canadian Patent #CA-1223932, July 7, 1987.

Several other published and non-published applications pending.

Journal Publications

- Leung,K., Clark,M.V., McNair,B., Kostic,Z., Cimini,L.J., Winters,J.H., "Outdoor IEEE 802.11 Cellular Networks: Radio and MAC Design and Their Performance", *IEEE Transactions on Vehicular Technology*, Vol. 56, No. 5, pp. 2673-2684, September 2007.
- Chuang, J., Cimini, L., Li, G., Lin, L., McNair, B., Sollenberger, N., Suzuki, M., Zhao, H., "High Speed wireless data access based on combining EDGE with wideband OFDM," *IEEE Communication Magazine*, November, 1999.
- D'Angelo, D.M., McNair, B., Wilkes, J.E., "Security in Electronic Messaging Systems," *AT&T Technical Journal*, Volume 73, Number 3, 1994.

Research awards

- "Standalone/Networked Compact, Low Power, Image-fused Multi-Spectrum Sensor System for Target Acquisition, Tracking and Fire Control," ARDEC, $2365000, co-PI with Victor Lawrence, Hong Man. AY2008-2009
- NSF: "REU Site: Integrated Software Radio and Radio Frequency Test Bed for Wireless Research in Dynamic Spectrum Access"; $296,754; NSF; Co-PI with Yu-Dong Yao. AY2004-2005
- AT&T Labs-Research Equipment donation of $900k DSP systems and wireless test equipment. AY2003-2004
- AT&T Labs-Research - $60k grant for "Investigation of Broadband Powerline technology" AY2003-2004

Masters theses supervised

- Xiongwei Xu, "The synchronization of IEEE 802.11A System", May 2014.
- Abdurazak Fathalla, "Security of Cloud Computing," May 2011.
- Tejas Marathe, "Comprehensive Performance Criteria for Wi-Fi Location Systems," December 2008.

Masters theses supervised (continued)

- Milin Patel, “Network Performance Enhancement using QoS, TCP Optimization, Application Acceleration and Dynamic Resource Allocation Techniques,” January 2008.
- Leo Gerard Raj, “Security in 4G Wireless Systems,” May 2005.

PhD committees

- Chao Tian, “Realization of Pure AM/FM Modulation via Combined Optical and Electrical Injection of Carriers in DFB Laser,” Stevens Institute of Technology, Physics Department, March 2015.
- Tao Yang, “All-optical frequency modulation of quantum cascade laser and its application on infrared spectroscopy,” Stevens Institute of Technology, Physics Department, May 2014.
- Fangming He, “Physical Security in Wireless Communications,” Stevens Institute of Technology, Electrical and Computer Engineering Department, May, 2012.
- Vinod Challa, “Vibration Energy Harvesting for Low Power and Wireless Applications,” Stevens Institute of Technology, Mechanical Engineering Department, May, 2011.
- Brian Borowski, “Application of Channel Estimation to Underwater Acoustic Communication,” Stevens Institute of Technology, Computer Science Department, June, 2010.
- Gang Chen, "All-Optical Modulation of Quantum Structure/Devices," Stevens Institute of Technology, Physics Department, May 2010.

Conference Papers

- He, F., Man, H., Kivanc, D., McNair, B., “EPSON: Enhanced Physical Security in OFDM Networks,” Proc. ICC 2009, Dresden, Germany, June 2009.
- Patel, S.; Cimini Jr, L.J.; McNair, B., “Comparison of frequency offset estimation techniques for burst OFDM,” *Proc. IEEE Vehicular Technology Conference VTC2002*, Birmingham, AL, May, 2002.
- Cimini, L., Leung, K., McNair, B., Winters, J. "Outdoor IEEE 802.11b Cellular Networks: MAC Protocol Design and Performance," *Proc. ICC 2002*, New York, NY, April 2002
- Clark, M., Leung, K., McNair, B., Kostic, Z., "Outdoor IEEE 802.11b Cellular Networks: Radio Link Performance", *Proc. ICC 2002*, New York, NY, April 2002.
- McNair, B., “Software Radio – the Commercial Perspective,” *Proc. IEEE Sarnoff Symposium*, Princeton, NJ, March 2002.
- Zou, H., Daneshard, B., McNair, B., "An Integrated OFDM Receiver for High-Speed Mobile Data Communications," *Proc. IEEE Globecom 2001*, San Antonio, TX, Oct. 2001.
- McNair, B., "Future Directions for Wireless Communications," *Supercomm2001*, Atlanta, GA, June, 2001

Conference Papers (continued)

- Cimini, L., McNair, B, "OFDM for High Data Rate, High-Mobility, Wide-Area Wireless Communications," *Proc. IEEE Sarnoff Symposium*, Princeton, NJ, March, 2001.
- Cimini, L., McNair, B, Sollenberger, N., "Implementation of an Experimental 384 kb/s Radio Link for High-Speed Internet Access," *Proc. IEEE Vehicular Technology Conference VTC2000*, Boston, MA, September, 2000.
- Cimini, L., McNair, B, Sollenberger, N., "Performance of an Experimental 384 kb/s 1900 MHz Radio Link In a Wide-Area High-Mobility Environment," *Proc. IEEE Vehicular Technology Conference VTC2000*, Boston, MA, September, 2000.
- Takamura, K.; Kunihiro, T.; Yamaura, T.; Fujita, E.; Anderson, G.; Chibane, C.; Feinberg, P.; Sollenberger, N.; McNair, B.; Mielcarek, E., "Field trial results of a band hopping OFDM system,' *Proc. IEEE Vehicular Technology Conference VTC99-Fall*, 1999. Amsterdam, the Netherlands, September 1999.
- McNair, B., Cimini, L., Sollenberger, N., "A Robust Timing and Frequency Offset Estimation Scheme for Orthogonal Frequency Division Multiplexing (OFDM) Systems," *Proc. IEEE Vehicular Technology Conference, VTC99*, Houston, TX, May 1999.
- McNair, B., Gupta, S., Kostic, Z., Sollenberger, N., "Experimental Results for Extensions to the IS-136 TDM Standard Based on Higher Level Modulation, Coherent Detection, and Equal Gain Antenna Combining," *Proc. IEEE Vehicular Technology Conference, VTC99*, Houston, TX, May 1999.
- Kostic, Z., McNair, B., Sollenberger N., "Experimental Performance Results of an Indoor Wireless Extension of IS-136 Based on pi/8 D8PSK, Coded Modulation, and Antenna Diversity," *Proc. IEEE Vehicular Technology Conference, VTC98*, Ottawa, Canada, May 1998.
- McNair, B., "The Effectiveness of Preselection Diversity for Indoor Wireless Systems," Proc. Int. Conf. on Universal Personal Communications, San Diego, CA, Oct. 1997.

Invited talks

- "Adventures in On-Line Education," Tsinghua University Webinar: Showcasing Online Course Designs, Online Teaching Guidance Expert Group, International Center for Engineering Educations (ICEE) – The United Nations Educational, Scientific and Cultural Organization (UNESCO), April 27, 2020.
- "Providing Structure, Motivation and Process in Security Education," Stevens/NIKSUN Workshop on Innovations in Cyber Security Research, Education and Training, Hoboken, NJ, March 2015
- "Wireless Security Panel," IEEE/AFCEA Fort Monmouth Annual Information Technology Forum and Expo, April 2005.

Invited talks (continued)

- "Of What Use is Wireless Multimedia Without Security," "What's Next in Multimedia Panel," 14th Annual Wireless and Optical Communications Conference, April 2005.
- "Is Wireless Security an Oxymoron?" IEEE Princeton/Central NJ Communications and Consumer Electronics and Computer Science Chapters, December, 2003.

Other Publications

- McNair, B., "Automatic Repeater Offsets," *73 Magazine,* November 1978, pp. 82-86.
- McNair, B, Williman, G., "Digital Keyboard Entry System," *Ham Radio,* Volume 11, Number 9, September, 1978, pp. 92-97.
- McNair, B., "A Digital Display for Amateur Radio Communications Equipment," *Ham Radio,* Volume 9, Number 9, September 1976, pp. 16-25.
- MIL-STD-188-114, "Electrical Characteristics of Digital Interface Circuits," Department of Defense Interface Standard, 24 March 1976

- Graduate:
  - EE/CpE-517 - Digital and Computer Systems Architecture (on-campus)
  - EE/TM/NIS-584 – Wireless System Security (on-campus and on-line)
  - EE-585/PEP-685/MT-685 – Physical Design of Wireless Communications (on-campus and on-line)
  - NiS/CpE-691 – Information Systems Security (on-campus and on-line)
  - EE/CpE-810A - Special Topics in EE/CpE - Digital and Computer Systems Architecture (on-campus)

- Undergraduate (on-campus):
  - E-232 – Design IV
  - BME-322 – Biomedical Design VI
  - EE/CpE-322 – ECE Design VI
  - EE/CpE-345 – Modeling and Simulation
  - CpE-358/CS-381 –Switching Theory and Logical Design
  - EE-359 – Electronic Circuits
  - EE/CpE-423; EE/CpE-424 – Senior Design
  - CpE-450 – Real-time Embedded Systems

Short Courses

- “Electronics and Computers,” preparation course for Fundamentals of Engineering/Professional Engineering license
  Stevens Institute of Technology
- "Digital Signal Processing - Principles, Architecture, and System Applications"
  - *Organizational Effectiveness Institute (originally Johns Hopkins University's continuing education program)*,
- "Wireless Digital Communications Systems: Components, Specifications, Test and Evaluation"
  - *Organizational Effectiveness Institute*
- "Security in Digital Communications Networks"
  - *Bell Labs Architecture Area Adopt a University Program: Grambling State University*
  - *Monmouth University*
- “Digital Telephony"
  - *Monmouth University*
  - *Fort Monmouth Education Center*
  - *Berlin (F.R.G.) Continuing Engineering Education Program*
- "Digital Communications & Applications"
  - *University of Maryland*
  - *Fort Monmouth Education Center*
  - *UCLA Extension University*
- "Digital Communications," presented with Allen Gersho, N.S. Jayant and David Falconer.
  - *George Washington University*
- "Data Communications for the System Designer"
  - *Bell Labs In-Hours Continuing Education Program*

Expert witness, patent consulting experience

- Authentication technology
- Bluetooth, WiFi, ZigBee, and other local/personal area wireless networking
- Cellular systems
- Communications networking
- Digital clock control for power management in SoCs
- Digital Rights Management
- Digital Subscriber Loop (DSL) technology
- Electronic technology
- Embedded systems
- Emergency alerting systems
- Geolocation technology
- Industrial process control software
- Localization services
- Messaging systems
- Multifactor Authentication
- Peer-to-peer and client-server networks
- Secure voice communications
- Signal processing
- Smart cards and magnetic stripe cards for payment systems
- Software/firmware code analysis (C, VHDL)
- Software trade secrets
- Television and television tuner technology
- Trusted systems
- User and system authentication technology
- Video messaging
- Video scrambling and pay-per-view systems
- Voice processing and voice response systems
- Wireless communications and networking – particularly PHY and MAC layers

Law firms supported

- Alston-Bird, New York, NY and Charlotte, NC (Kirk Bradley, Darlena Subashi, Karlee Wroblewski)
- Baker & McKenzie, Dallas, TX (William McSpadden)
- Bradley, Birmingham, AL (Paul Sykes, Benn Wilson, Jake Gipson)
- Bragalone-Conroy, Dallas, TX (Nick Kliewer, Daniel Olejko, Stephanie Wood)
- Cantor-Colburn, Hartford, CT (Steve Coyle)
- Carella-Byrne (Donald Ecklund)
- Clark-Hill, Pittsburgh, PA, (J. Alexander Hershey)
- Desmarias, New York, NY (Kerri-Ann Leembeck)
- DLA Piper, Austin, TX, San Francisco, CA and San Diego, CA (Brian Erickson, Gerald Sekimura, Kevin Hamilton)
- Fox Rothschild, Lawrenceville, NJ (Gerard Norton)
- Gibbons-Deldeo, Newark, NJ (Michael Cukor, Sheila McShane, Vin McGeary, Erich Falke, Chris Strate)
- Goodwin-Proctor, New York, NY and Washington, DC. (Mark Abate, Calvin Wingfield)
- Greenberg-Traurig, McLean, VA (Andrew Sommer)
- Hogan-Lovells, Denver, CO (Matt Rozier, Aaron Oakley, Lucky Vidmar)
- Jones-Day, New York, NY (Tom Gianetti)
- Latimer, LLP, Oakhurst, NJ (Brian Latimer)
- Merchant-Gould, Atlanta, GA (George Jenson)
- Morrison-Foerster, San Diego, CA (Christian Andreau-von Eaw)
- Oblon Spivak, Arlington, VA (Robert Mattson, Scott McKeown)
- Orrick, Herrington and Sutcliffe, Silicon Valley (Jason Angell)
- Quattlebaum, Grooms, Tull & Burrow, Little Rock, AR (Steve Quattlebaum)
- Quinn-Emanuel, New York, NY (Marc Kaplan)
- Ropes & Gray, Washington, DC, (Scott McKeown, Victor Cheung)
- Sabety & Associates (Ted Sabety)
- Sidley Austin, Chicago, IL, Washington, D.C. (Doug Lewis, Rick Cederoth, Mike Franzinger)
- Steptoe & Johnson, Washington, D.C. (Kate Cappaert, Brian Johnson)
- Carr & Waddoups, Salt Lake City, UT (Trent Waddoups)
- Unified Patents, Washington, DC (Michelle Callaghan/Aspen, Ashraf Fawzy, Jung Hahm, Roshan Mansinghani, Jessica Marks, Jordan Rossen, David Seastrunck)
- Wilson, Sonsini, Goodrich & Rosati, Palo Alto, CA, Seattle, WA (Matthew Argenti, Quincy Lu)
- White Case, Washington, DC, New York, NY (David Tennant, Grace Wang)
- Wisser and Weinstein, West Hartford, CT (Kerry Wisser)
- Woodcock and Washburn, Philadelphia, PA (Michael Bonella)

APPENDIX B

(Documents Considered)

Exhibit ("Ex.")	Description
1001	U.S. Patent No. 10,692,340
1002	File History of U.S. Application No. 16/200,172, which led to U.S. Patent No. 10,692,340
1009	U.S. Patent Application Publication No. 2016/0247370 to Lamb
1010	U.S. Patent No. 6,057,764 to Williams
1011	U.S. Patent No. 7,696,873 to Sharma