US007230528B2

(12) **United States Patent**
Kates

(10) **Patent No.: US 7,230,528 B2**
(45) **Date of Patent: Jun. 12, 2007**

(54) **PROGRAMMED WIRELESS SENSOR SYSTEM**

(76) Inventor: **Lawrence Kates**, 1111 Bayside Dr., Corona Del Mar, CA (US) 92625

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **11/231,321**

(22) Filed: **Sep. 20, 2005**

(65) **Prior Publication Data**

US 2007/0063833 A1 Mar. 22, 2007

(51) **Int. Cl.**
G08B 19/00 (2006.01)
G08B 1/08 (2006.01)

(52) **U.S. Cl.** **340/521**; 340/539.19; 340/825.36; 340/825.49; 340/825.69

(58) **Field of Classification Search** 340/521, 340/539.19, 539.16, 539.17, 539.18, 539.14
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,099,168	A	7/1978	Kedjierski
4,136,823	A	1/1979	Kullberg
4,226,533	A	10/1980	Snowman
4,266,220	A	5/1981	Malinowski
4,400,694	A	8/1983	Wong et al.
4,420,746	A	12/1983	Malinowski
4,455,553	A	6/1984	Johnson
4,535,450	A	8/1985	Tan
4,543,570	A	9/1985	Bressert et al.
4,556,873	A	12/1985	Yamada et al.
4,652,859	A	3/1987	Van Wienen
4,661,804	A	4/1987	Abel
4,670,739	A	6/1987	Kelly, Jr.
4,675,661	A	6/1987	Ishii
4,692,742	A	9/1987	Raizen et al.

(Continued)

FOREIGN PATENT DOCUMENTS

EP 0 346 152 A2 12/1989

(Continued)

OTHER PUBLICATIONS

"Measuring and Controlling Indoor Humidity," http://www.relative-humidity-sensor.com, 3 pages, Jun. 18, 2004.

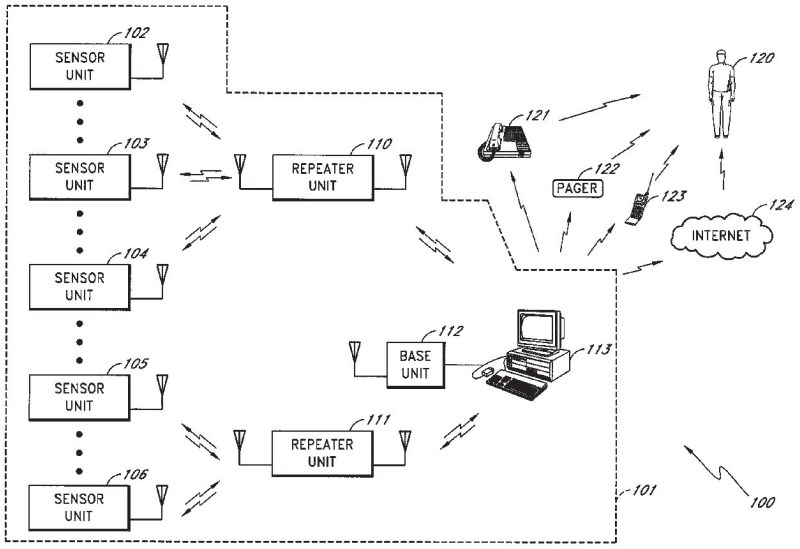
(Continued)

Primary Examiner—Donnie L. Crosland
(74) *Attorney, Agent, or Firm*—Knobbe, Martens, Olson & Bear, LLP

(57) **ABSTRACT**

A low cost, robust, wireless sensor system that provides an extended period of operability without maintenance is described. The system includes one or more intelligent sensor units and a base unit that can communicate with a large number of sensors. When one or more of the sensors detects an anomalous condition (e.g., smoke, fire, water, etc.) the sensor communicates with the base unit and provides data regarding the anomalous condition. The base unit can contact a supervisor or other responsible person by a plurality of techniques, such as, telephone, pager, cellular telephone, Internet, etc. In one embodiment, one or more wireless repeaters are used between the sensors and the base unit to extend the range of the system and to allow the base unit to communicate with a larger number of sensors. In one embodiment, each sensor is labeled according to its intended location, and system configuration data containing the sensor identification codes and corresponding sensor locations is provided to the user.

30 Claims, 9 Drawing Sheets



ecobee Exhibit 1021
ecobee v. Ollnova

U.S. PATENT DOCUMENTS

4,692,750	A		9/1987	Murakami et al.
4,727,359	A		2/1988	Yuchi et al.
4,801,865	A		1/1989	Miller et al.
4,827,244	A		5/1989	Bellavia et al.
4,862,514	A		8/1989	Kedjierski
4,871,999	A		10/1989	Ishii et al.
4,901,316	A		2/1990	Igarashi et al.
4,916,432	A		4/1990	Tice et al.
4,939,504	A		7/1990	Miller
4,951,029	A	*	8/1990	Severson 340/506
4,977,527	A		12/1990	Shaw et al.
4,996,518	A		2/1991	Takahashi et al.
5,134,644	A		7/1992	Garton et al.
5,138,562	A		8/1992	Shaw et al.
5,151,683	A		9/1992	Takahashi et al.
5,159,315	A		10/1992	Schulz et al.
5,168,262	A		12/1992	Okayama
5,229,750	A		7/1993	Welch, Jr. et al.
5,260,687	A		11/1993	Yamauchi et al.
5,267,180	A		11/1993	Okayama
5,281,951	A		1/1994	Okayama
5,315,291	A		5/1994	Furr
5,319,698	A		6/1994	Glidewell et al.
5,335,186	A	*	8/1994	Tarrant 702/127
5,345,224	A		9/1994	Brown
5,359,241	A		10/1994	Hasegawa et al.
5,400,246	A		3/1995	Wilson et al.
5,430,433	A		7/1995	Shima
5,432,500	A		7/1995	Scripps
5,530,433	A		6/1996	Morita
5,568,121	A		10/1996	Lamensdorf
5,574,435	A		11/1996	Mochizuki
5,627,515	A		5/1997	Anderson
5,655,561	A		8/1997	Wendel et al.
5,736,928	A		4/1998	Tice et al.
5,748,092	A		5/1998	Arsenault et al.
5,854,994	A	*	12/1998	Canada et al. 702/56
5,859,536	A		1/1999	Stockton
5,881,951	A		3/1999	Carpenter
5,889,468	A		3/1999	Banga
5,907,491	A		5/1999	Canada et al.
5,923,102	A		7/1999	Koenig et al.
5,949,332	A		9/1999	Kim
6,025,788	A		2/2000	Diduck
6,031,455	A		2/2000	Grube et al.
6,049,273	A		4/2000	Hess
6,060,994	A		5/2000	Chen
6,075,451	A		6/2000	Lebowitz et al.
6,078,050	A		6/2000	Castleman
6,078,269	A		6/2000	Markwell et al.
6,084,522	A		7/2000	Addy
6,097,288	A		8/2000	Koeppe, Jr.
6,175,310	B1		1/2001	Gott
6,208,247	B1	*	3/2001	Agre et al. 340/539.19
6,215,404	B1		4/2001	Morales
6,313,646	B1		11/2001	Davis et al.
6,320,501	B1		11/2001	Tice et al.
6,369,714	B2		4/2002	Walter
6,377,181	B1		4/2002	Kroll et al.
6,380,860	B1		4/2002	Goetz
6,420,973	B2		7/2002	Acevedo
6,437,692	B1		8/2002	Petite et al.
6,441,731	B1		8/2002	Hess
6,445,292	B1		9/2002	Jen et al.
6,489,895	B1		12/2002	Apelman
6,515,283	B1		2/2003	Castleman et al.
6,526,807	B1		3/2003	Doumit et al.
6,552,647	B1		4/2003	Thiesen et al.
6,553,336	B1	*	4/2003	Johnson et al. 702/188
6,583,720	B1		6/2003	Quigley
6,704,681	B1		3/2004	Nassof et al.
6,731,215	B2		5/2004	Harms et al.
6,748,804	B1		6/2004	Lisec et al.
6,759,956	B2		7/2004	Menard
6,796,187	B2		9/2004	Srinivasan et al.
6,798,220	B1		9/2004	Flanigan et al.
6,940,403	B2		9/2005	Kail, IV
6,995,676	B2		2/2006	Amacher
2002/0011570	A1		1/2002	Castleman
2002/0033759	A1		3/2002	Morello
2002/0186141	A1		12/2002	Jen et al.
2003/0011428	A1		1/2003	Yamakawa et al.
2003/0058093	A1		3/2003	Dohi et al.
2003/0122677	A1		7/2003	Kail, IV
2003/0199247	A1		10/2003	Striemer
2004/0007264	A1		1/2004	Bootka
2005/0105841	A1		5/2005	Luo et al.
2005/0116667	A1		6/2005	Mueller et al.
2005/0128067	A1		6/2005	Zakrewski
2005/0131652	A1		6/2005	Corwin et al.

FOREIGN PATENT DOCUMENTS

EP	0 346 152 A3	12/1989
WO	WO 00-21047 A1	4/2000
WO	WO 2004-010398 A1	1/2004
WO	WO 2004-073326 A2	8/2004

OTHER PUBLICATIONS

"Impedance Moisture Sensor Technology," http://www.sensorland.com/HowPage029.html, 2 pages, Jun. 18, 2004.

"Relative Humidity Information," www.relative-humidity-sensor.com/relative-humidity.html 6 pages, Jun. 18, 2004.

"Ways to Prevent Mold Problems," http://www.toxic-black-mold-info.com/prevent.html, 12 pages, Jun. 18, 2004.

"G-Cap™ 2 Relative Humidity Sensor," http://www.globalspec.com/FeaturedProducts/Detail?ExhibitID=1454, 2 pages, Jun. 18, 2004.

Texas Instruments, Inc., Product catalog for "TRF6901 Single-Chip RF Transceiver," Copyright 2001-2003, 27 pages.

Texas Instruments, Inc., Mechanical Data for PT (SPQFP-G48) Plastic Quad Flatpack, 2 pages, Jan. 2004.

"Waterbug" Data Sheet, Model WB-200, www.winland.com, 2 pages Aug. 16, 2006.

* cited by examiner

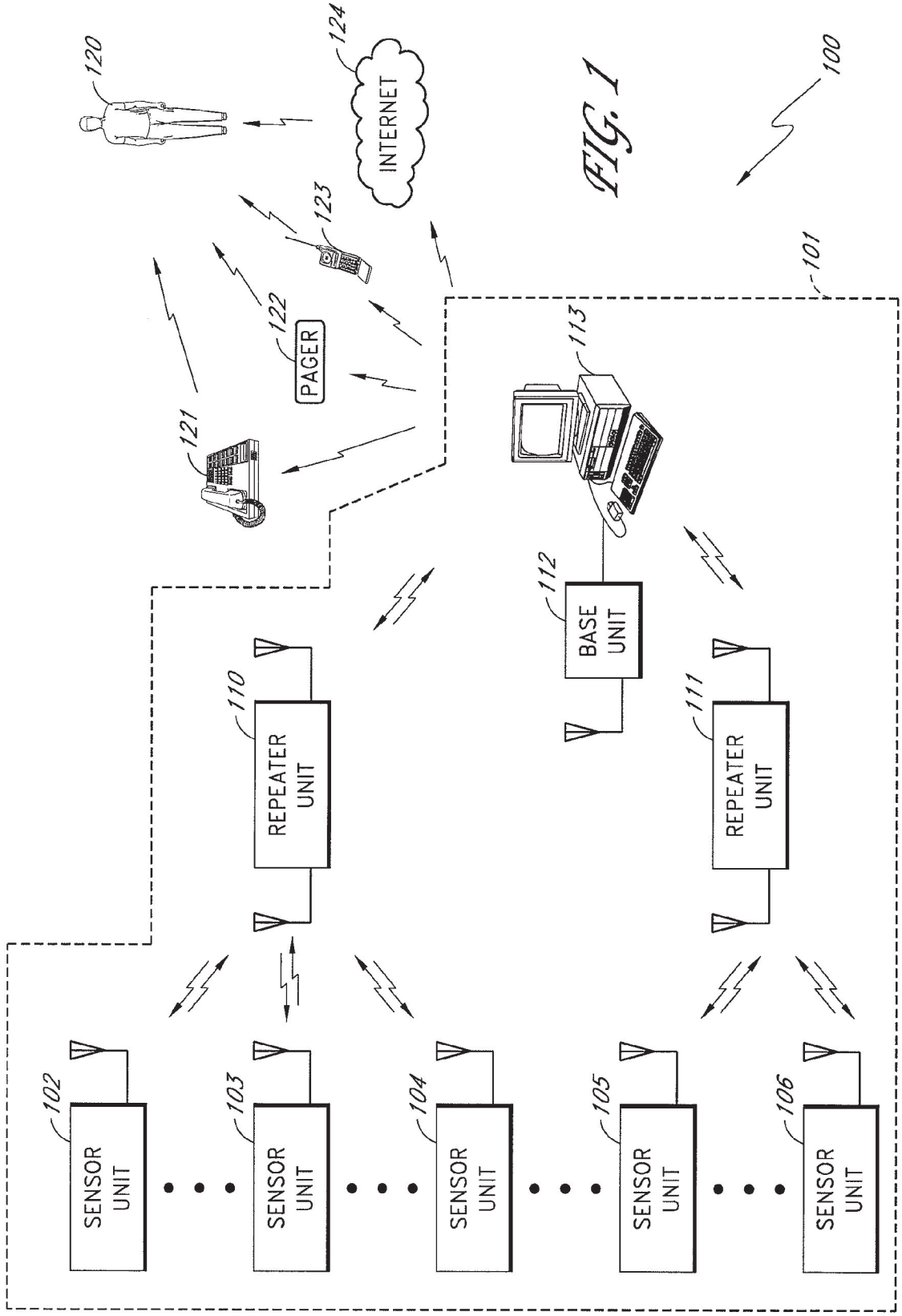

120
124
INTERNET
100
123
101
122
PAGER
113
121
112
BASE UNIT
110
REPEATER UNIT
111
REPEATER UNIT
102
SENSOR UNIT
103
SENSOR UNIT
104
SENSOR UNIT
105
SENSOR UNIT
106
SENSOR UNIT

FIG. 1

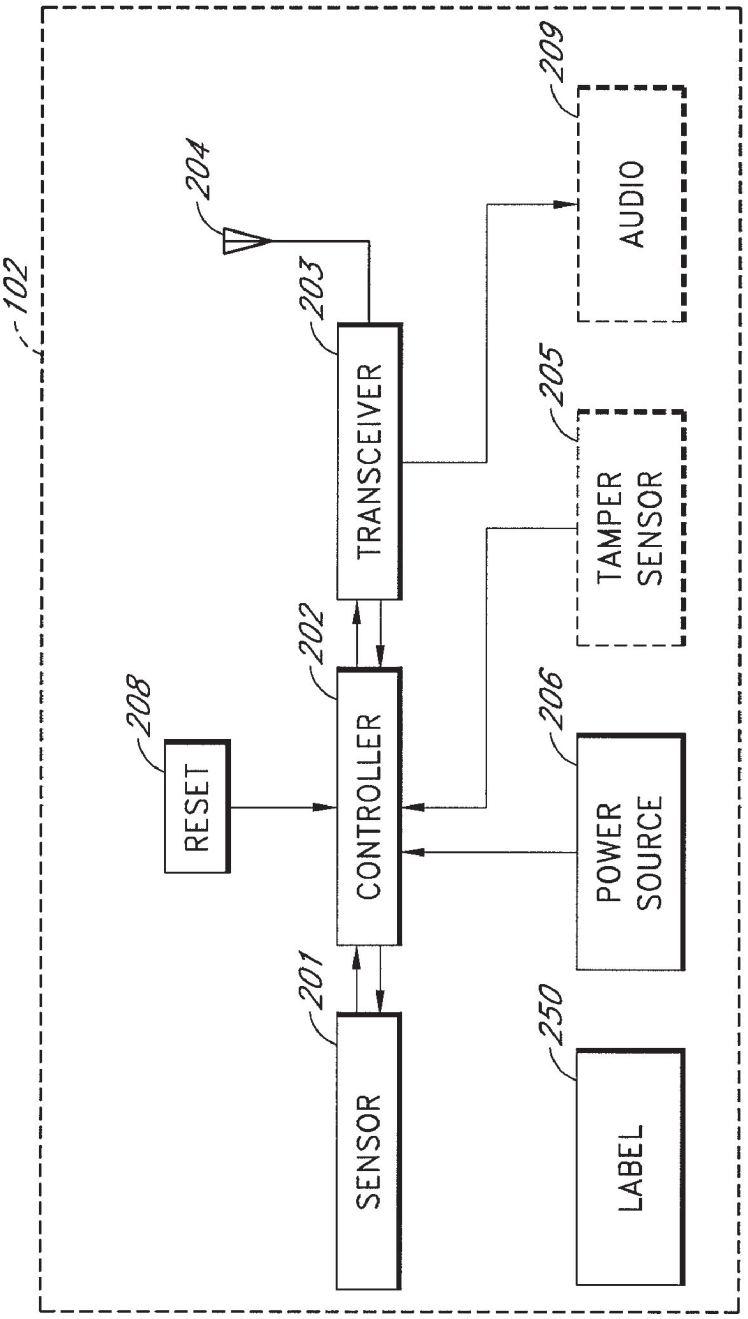

102
204
203
209
AUDIO
TRANSCEIVER
205
TAMPER SENSOR
202
208
RESET
CONTROLLER
206
POWER SOURCE
201
SENSOR
250
LABEL
SENSOR UNIT

FIG. 2

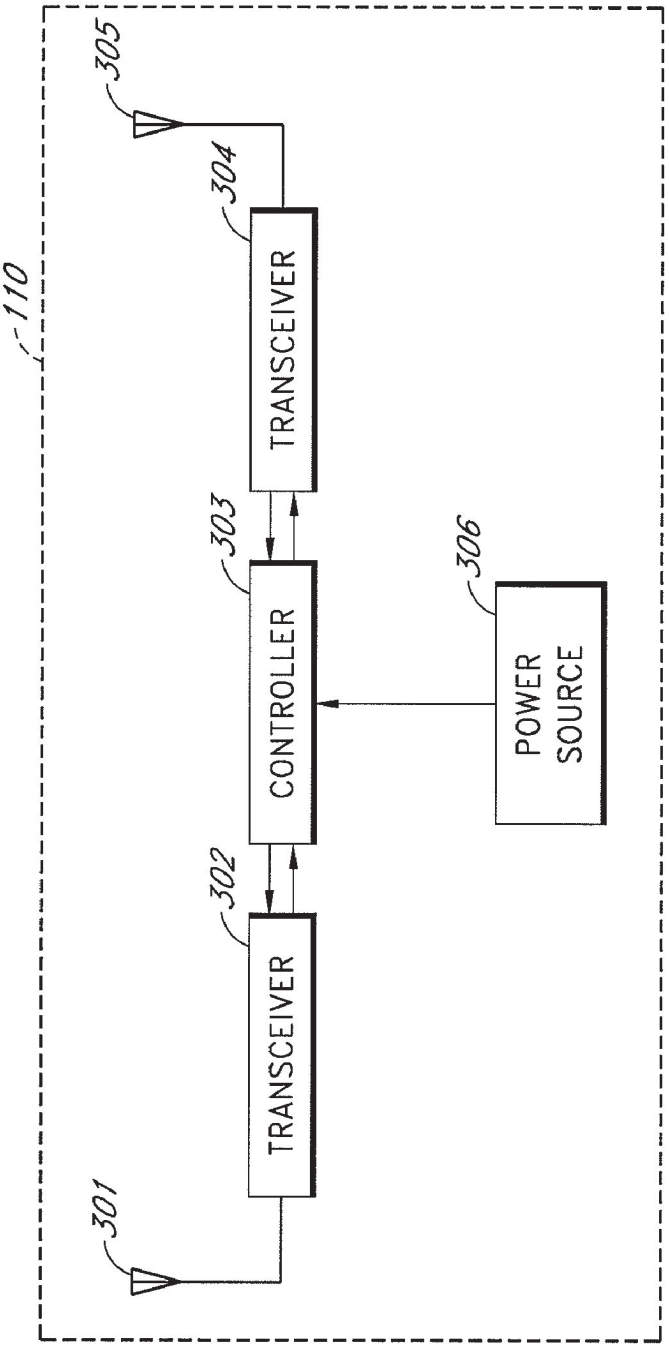

110
305
304
TRANSCEIVER
303
CONTROLLER
306
POWER SOURCE
302
TRANSCEIVER
301

FIG. 3

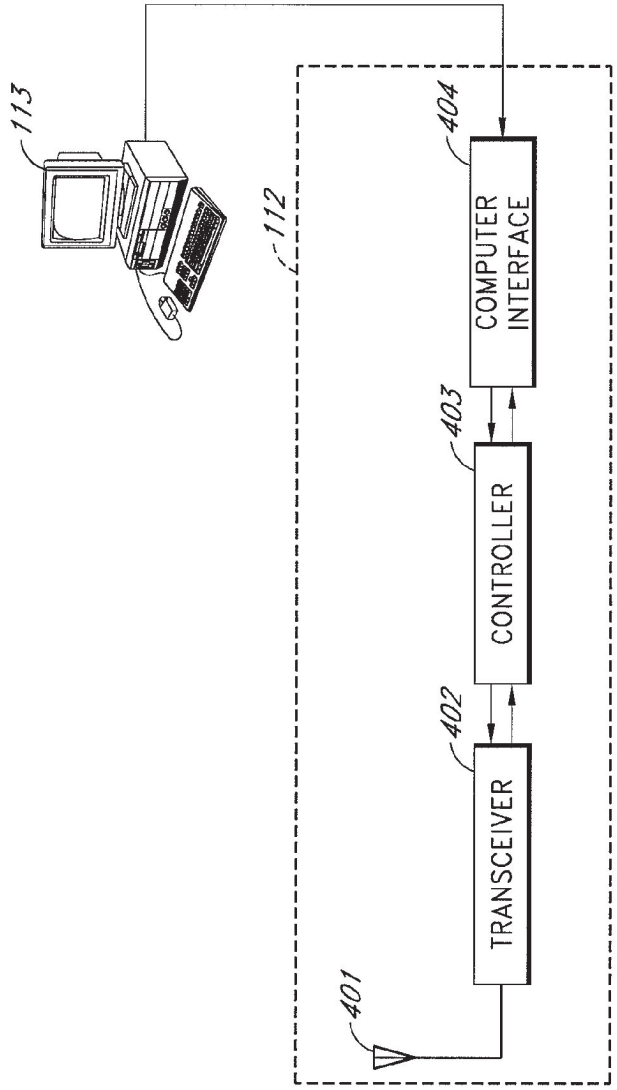

113
112
404
COMPUTER INTERFACE
403
CONTROLLER
402
TRANSCEIVER
401

FIG. 4

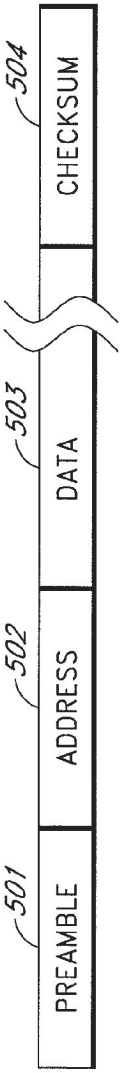

504
CHECKSUM
503
DATA
502
ADDRESS
501
PREAMBLE

FIG. 5

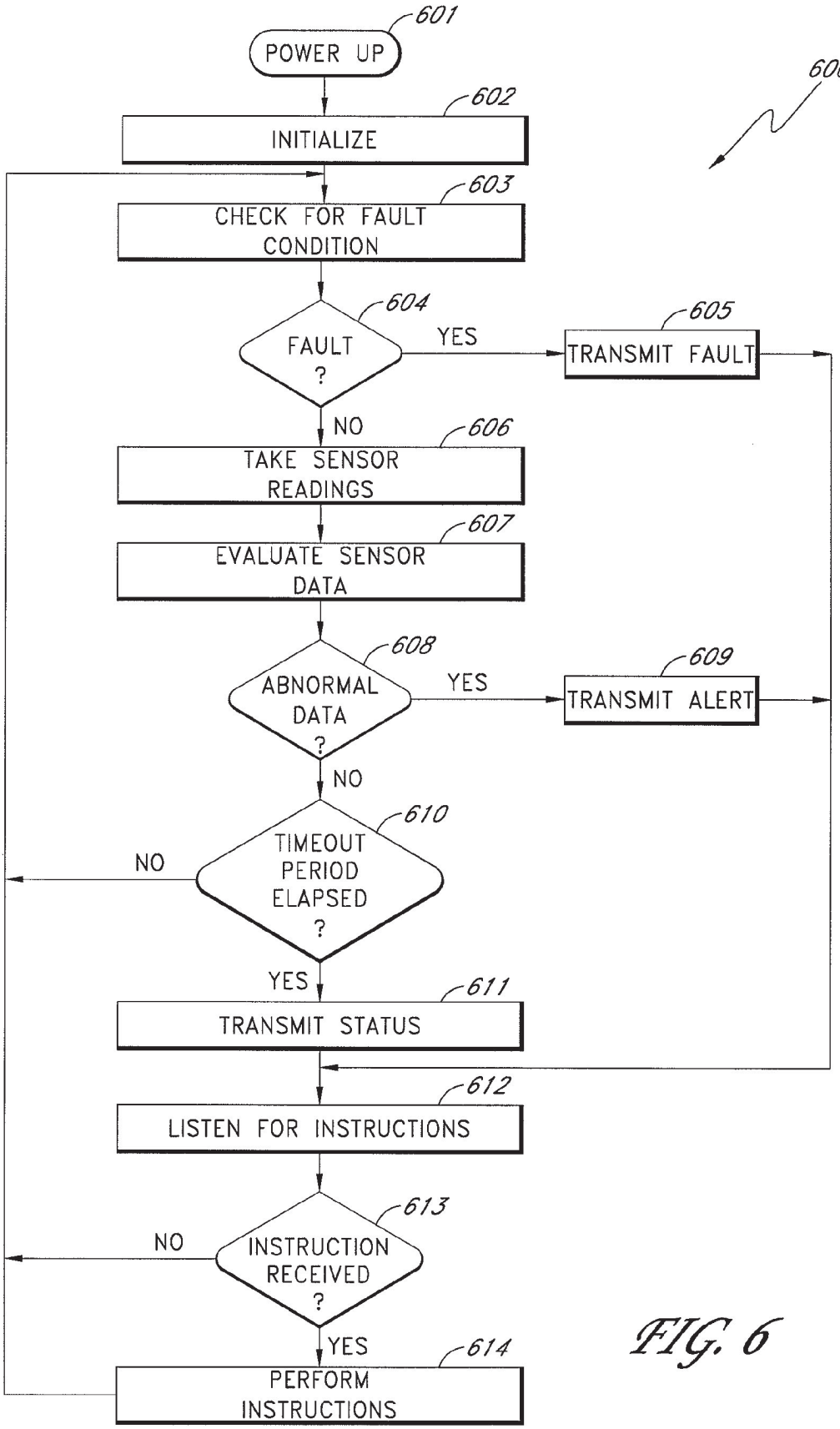

601
POWER UP
600
602
INITIALIZE
603
CHECK FOR FAULT CONDITION
604
FAULT ?
YES
605
TRANSMIT FAULT
NO
606
TAKE SENSOR READINGS
607
EVALUATE SENSOR DATA
608
ABNORMAL DATA ?
YES
609
TRANSMIT ALERT
NO
610
TIMEOUT PERIOD ELAPSED ?
NO
YES
611
TRANSMIT STATUS
612
LISTEN FOR INSTRUCTIONS
613
INSTRUCTION RECEIVED ?
NO
YES
614
PERFORM INSTRUCTIONS

FIG. 6

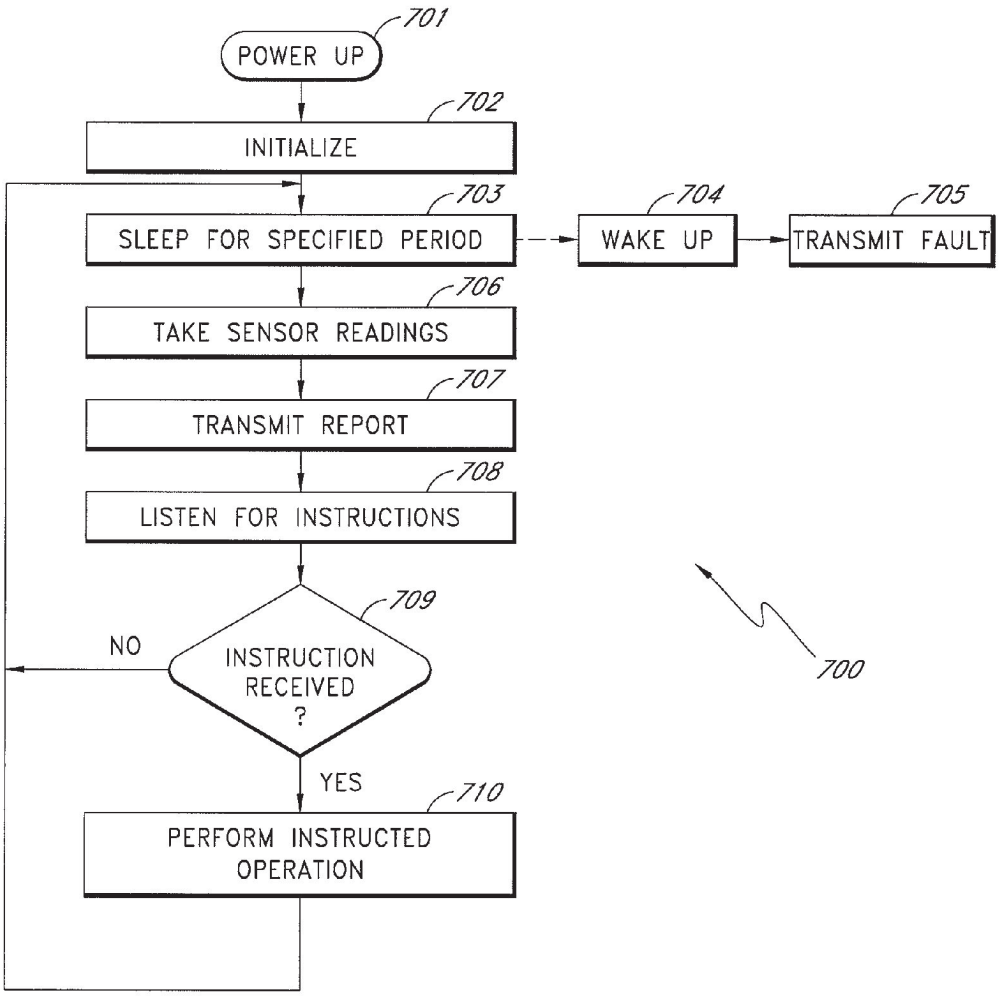

701
POWER UP
702
INITIALIZE
703
SLEEP FOR SPECIFIED PERIOD
704
WAKE UP
705
TRANSMIT FAULT
706
TAKE SENSOR READINGS
707
TRANSMIT REPORT
708
LISTEN FOR INSTRUCTIONS
709
INSTRUCTION RECEIVED ?
NO
YES
710
PERFORM INSTRUCTED OPERATION
700

FIG. 7

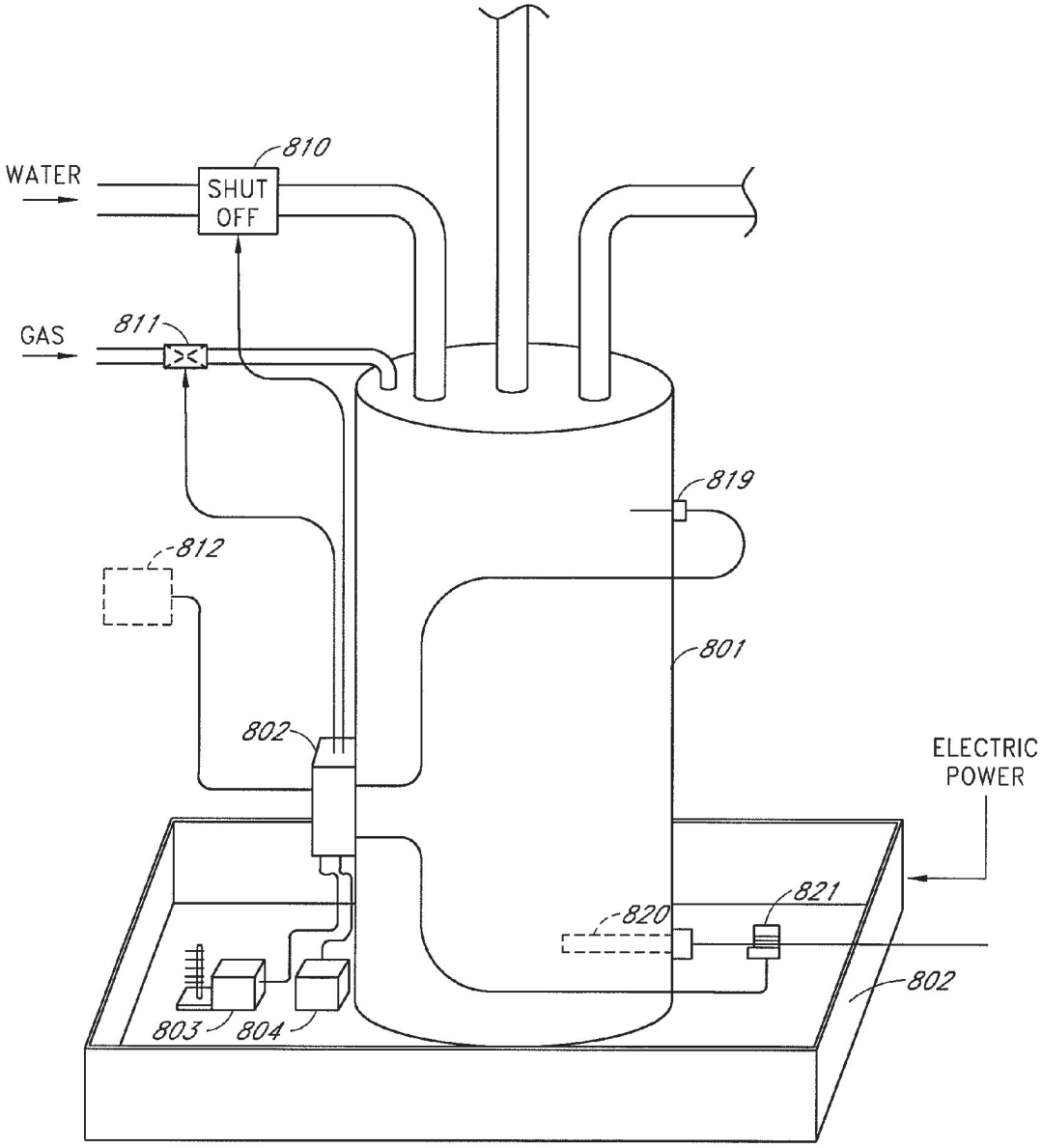

WATER
SHUT OFF
810
GAS
811
819
812
801
802
ELECTRIC POWER
821
820
802
803
804

FIG. 8

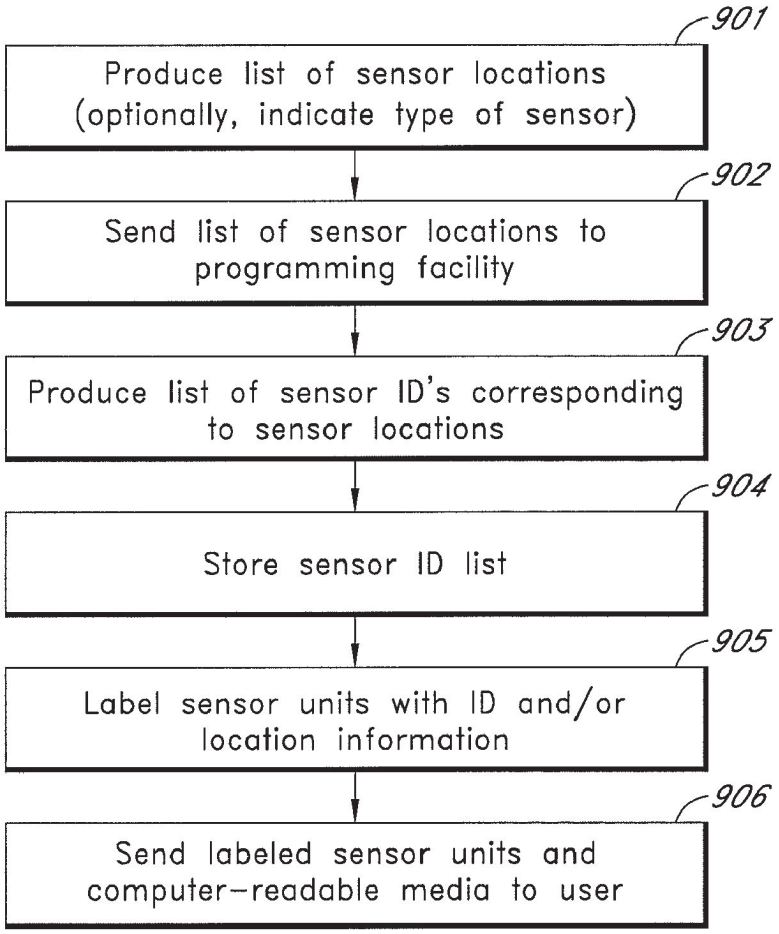

901
Produce list of sensor locations (optionally, indicate type of sensor)
902
Send list of sensor locations to programming facility
903
Produce list of sensor ID's corresponding to sensor locations
904
Store sensor ID list
905
Label sensor units with ID and/or location information
906
Send labeled sensor units and computer-readable media to user

FIG. 9

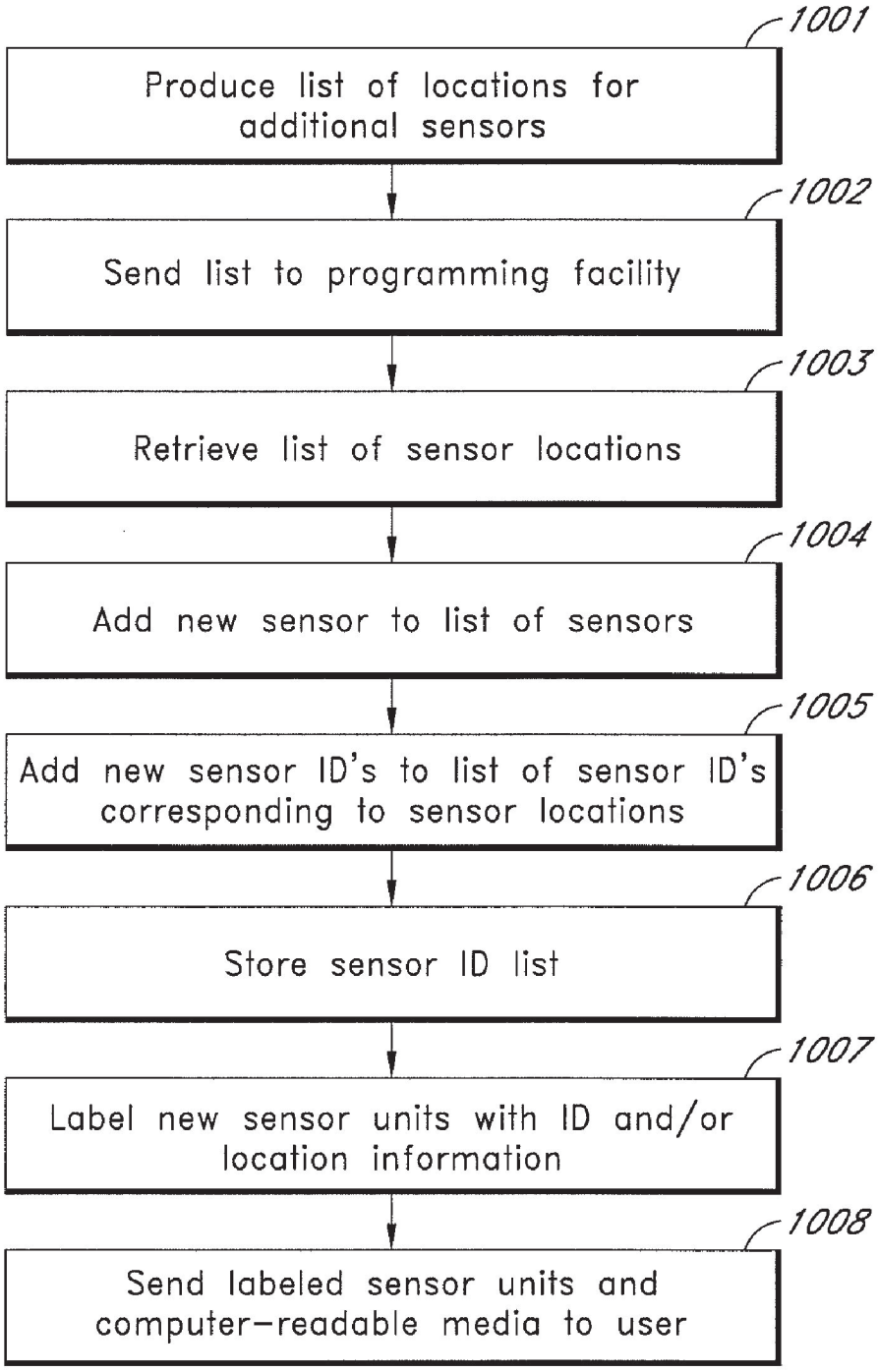

1001
Produce list of locations for additional sensors
1002
Send list to programming facility
1003
Retrieve list of sensor locations
1004
Add new sensor to list of sensors
1005
Add new sensor ID's to list of sensor ID's corresponding to sensor locations
1006
Store sensor ID list
1007
Label new sensor units with ID and/or location information
1008
Send labeled sensor units and computer-readable media to user

FIG. 10

PROGRAMMED WIRELESS SENSOR SYSTEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a wireless sensor system for monitoring potentially dangerous or costly conditions such as, for example, smoke, temperature, water, gas and the like in a building or vehicle, and/or for monitoring energy usage or efficiency of water heaters and the like.

2. Description of the Related Art

Maintaining and protecting a building or complex is difficult and costly. Some conditions, such as fires, gas leaks, etc., are a danger to the occupants and the structure. Other malfunctions, such as water leaks in roofs, plumbing, etc., are not necessarily dangerous for the occupants, but can, nevertheless, cause considerable damage. In many cases, an adverse condition such as water leakage, fire, etc., is not detected in the early stages when the damage and/or danger is relatively small. Sensors can be used to detect such adverse conditions, but sensors present their own set of problems. For example, adding sensors, such as, for example, smoke detectors, water sensors, and the like, in an existing structure can be prohibitively expensive due to the cost of installing wiring between the remote sensors and a centralized monitoring device used to monitor the sensors. Adding wiring to provide power to the sensors further increases the cost. Moreover, with regard to fire sensors, most fire departments will not allow automatic notification of the fire department based on the data from a smoke detector alone. Most fire departments require that a specific temperature rate-of-rise be detected before an automatic fire alarm system can notify the fire department. Unfortunately, detecting fire by temperature rate-of-rise generally means that the fire is not detected until it is too late to prevent major damage.

When a relatively large number of sensor units are used, as in, for example, a commercial building, apartment building, etc., then correlating an identification code in the sensor unit with a location of the sensor unit can become difficult. Correlating the location of a sensor unit with an identification code for the sensor unit can make it difficult to install and maintain the sensor system. Moreover, errors in correlating the location of the sensor unit with an identification code of the sensor unit can lead to potentially life-threatening delays when a sensor reports a dangerous condition and the report sensor cannot be located.

SUMMARY

The present invention solves these and other problems by providing a relatively low cost, robust, wireless sensor system wherein sensor units are labeled according to an intended location and computer-readable or networked data are provided to a monitoring system. The system provides an extended period of operability without maintenance. The system includes one or more intelligent sensor units and a base unit that can communicate with the sensor units. When one or more of the sensor units detects an anomalous condition (e.g., smoke, fire, water, etc.) the sensor unit communicates with the base unit and provides data regarding the anomalous condition. The base unit can contact a supervisor or other responsible person by a plurality of techniques, such as, telephone, pager, cellular telephone, Internet (and/or local area network), etc. In one embodiment, one or more wireless repeaters are used between the sensor units and the base unit to extend the range of the system and to allow the base unit to communicate with a larger number of sensors.

In one embodiment, the sensor system includes a number of sensor units located throughout a building that sense conditions and report anomalous results back to a central reporting station. The sensor units measure conditions that might indicate a fire, water leak, etc. The sensor units report the measured data to the base unit whenever the sensor unit determines that the measured data is sufficiently anomalous to be reported. The base unit can notify a responsible person such as, for example, a building manager, building owner, private security service, etc. In one embodiment, the sensor units do not send an alarm signal to the central location. Rather, the sensors send quantitative measured data (e.g., smoke density, temperature rate-of-rise, etc.) to the central reporting station.

In one embodiment, the sensor system includes a battery-operated sensor unit that detects a condition, such as, for example, smoke, temperature, humidity, moisture, water, water temperature, carbon monoxide, natural gas, propane gas, other flammable gases, radon, poison gasses, etc. The sensor unit is placed in a building, apartment, office, residence, etc. In order to conserve battery power, the sensor is normally placed in a low-power mode. In one embodiment, while in the low-power mode, the sensor unit takes regular sensor readings and evaluates the readings to determine if an anomalous condition exists. If an anomalous condition is detected, then the sensor unit "wakes up" and begins communicating with the base unit or with a repeater. At programmed intervals, the sensor also "wakes up" and sends status information to the base unit (or repeater) and then listens for commands for a period of time.

In one embodiment, the sensor unit is bi-directional and configured to receive instructions from the central reporting station (or repeater). Thus, for example, the central reporting station can instruct the sensor to: perform additional measurements; go to a standby mode; wake up; report battery status; change wake-up interval; run self-diagnostics and report results; etc. In one embodiment, the sensor unit also includes a tamper switch. When tampering with the sensor is detected, the sensor reports such tampering to the base unit. In one embodiment, the sensor reports its general health and status to the central reporting station on a regular basis (e.g., results of self-diagnostics, battery health, etc.).

In one embodiment, the sensor unit provides two wake-up modes, a first wake-up mode for taking measurements (and reporting such measurements if deemed necessary), and a second wake-up mode for listening for commands from the central reporting station. The two wake-up modes, or combinations thereof, can occur at different intervals.

In one embodiment, the sensor units use spread-spectrum techniques to communicate with the base unit and/or the repeater units. In one embodiment, the sensor units use frequency-hopping spread-spectrum. In one embodiment, each sensor unit has an Identification code (ID) and the sensor units attaches its ID to outgoing communication packets. In one embodiment, when receiving wireless data, each sensor unit ignores data that is addressed to other sensor units.

The repeater unit is configured to relay communications traffic between a number of sensor units and the base unit. The repeater units typically operate in an environment with several other repeater units and thus, each repeater unit contains a database (e.g., a lookup table) of sensor IDs. During normal operation, the repeater only communicates with designated wireless sensor units whose IDs appears in

the repeater's database. In one embodiment, the repeater is battery-operated and conserves power by maintaining an internal schedule of when its designated sensors are expected to transmit and going to a low-power mode when none of its designated sensor units is scheduled to transmit. In one embodiment, the repeater uses spread-spectrum to communicate with the base unit and the sensor units. In one embodiment, the repeater uses frequency-hopping spread-spectrum to communicate with the base unit and the sensor units. In one embodiment, each repeater unit has an ID and the repeater unit attaches its ID to outgoing communication packets that originate in the repeater unit. In one embodiment, each repeater unit ignores data that is addressed to other repeater units or to sensor units not serviced by the repeater.

In one embodiment, the repeater is configured to provide bi-directional communication between one or more sensors and a base unit. In one embodiment, the repeater is configured to receive instructions from the central reporting station (or repeater). Thus, for example, the central reporting station can instruct the repeater to: send commands to one or more sensors; go to standby mode; "wake up"; report battery status; change wake-up interval; run self-diagnostics and report results; etc.

The base unit is configured to receive measured sensor data from a number of sensor units. In one embodiment, the sensor information is relayed through the repeater units. The base unit also sends commands to the repeater units and/or sensor units. In one embodiment, the base unit includes a diskless PC that runs off of a CD-ROM, flash memory, DVD, or other read-only device, etc. When the base unit receives data from a wireless sensor indicating that there may be an emergency condition (e.g., a fire or excess smoke, temperature, water, flammable gas, etc.) the base unit will attempt to notify a responsible party (e.g., a building manager) by several communication channels (e.g., telephone, Internet, pager, cell phone, etc.). In one embodiment, the base unit sends instructions to place the wireless sensor in an alert mode (inhibiting the wireless sensor's low-power mode). In one embodiment, the base unit sends instructions to activate one or more additional sensors near the first sensor.

In one embodiment, the base unit maintains a database of the health, battery status, signal strength, and current operating status of all of the sensor units and repeater units in the wireless sensor system. In one embodiment, the base unit automatically performs routine maintenance by sending commands to each sensor to run a self-diagnostic and report the results. The bases unit collects such diagnostic results. In one embodiment, the base unit sends instructions to each sensor telling the sensor how long to wait between "wakeup" intervals. In one embodiment, the base unit schedules different wakeup intervals to different sensors based on the sensor's health, battery health, location, etc. In one embodiment, the base unit sends instructions to repeaters to route sensor information around a failed repeater.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** shows a sensor system that includes a plurality of sensor units that communicate with a base unit through a number of repeater units.

FIG. **2** is a block diagram of a sensor unit.

FIG. **3** is a block diagram of a repeater unit.

FIG. **4** is a block diagram of the base unit.

FIG. **5** shows one embodiment of network communication packet used by the sensor units, repeater units, and the base unit.

FIG. **6** is a flowchart showing operation of a sensor unit that provides relatively continuous monitoring.

FIG. **7** is a flowchart showing operation of a sensor unit that provides periodic monitoring.

FIG. **8** shows how the sensor system can be used to detected water leaks.

FIG. **9** is a flowchart showing one embodiment for configuring the sensor system by labeling sensor units according to an intended location and providing computer data to correlate a sensor identification code with a sensor location.

FIG. **10** is a flowchart showing one embodiment for adding sensors to an existing system.

DETAILED DESCRIPTION

FIG. **1** shows a sensor system **100** that includes a plurality of sensor units **102-106** that communicate with a base unit **112** through a number of repeater units **110-111**. The sensor units **102-106** are located throughout a building **101**. Sensor units **102-104** communicate with the repeater **110**. Sensor units **105-106** communicate with the repeater **111**. The repeaters **110-111** communicate with the base unit **112**. The base unit **112** communicates with a monitoring computer system **113** through a computer network connection such as, for example, Ethernet, wireless Ethernet, firewire port, Universal Serial Bus (USB) port, bluetooth, etc. The computer system **113** contacts a building manager, maintenance service, alarm service, or other responsible personnel **120** using one or more of several communication systems such as, for example, telephone **121**, pager **122**, cellular telephone **123** (e.g., direct contact, voicemail, text, etc.), and/or through the Internet and/or local area network **124** (e.g., through email, instant messaging, network communications, etc.). In one embodiment, multiple base units **112** are provided to the monitoring computer **113**. In one embodiment, the monitoring computer **113** is provided to more than one computer monitor, thus, allowing more data to be displayed than can conveniently be displayed on a single monitor. In one embodiment, the monitoring computer **113** is provided to multiple monitors located in different locations, thus, allowing the data from the monitoring computer **113** to be displayed in multiple locations.

The sensor units **102-106** include sensors to measure conditions, such as, for example, smoke, temperature, moisture, water, water temperature, humidity, carbon monoxide, natural gas, propane gas, security alarms, intrusion alarms (e.g., open doors, broken windows, open windows, and the like), other flammable gases, radon, poison gasses, etc. Different sensor units can be configured with different sensors or with combinations of sensors. Thus, for example, in one installation the sensor units **102** and **104** could be configured with smoke and/or temperature sensors while the sensor unit **103** could be configured with a humidity sensor.

The discussion that follows generally refers to the sensor unit **102** as an example of a sensor unit, with the understanding that the description of the sensor unit **102** can be applied to many sensor units. Similarly, the discussion generally refers to the repeater **110** by way of example, and not limitation. It will also be understood by one of ordinary skill in the art that repeaters are useful for extending the range of the sensor units **102-106** but are not required in all embodiments. Thus, for example in one embodiment, one or more of the sensor units **102-106** can communicate directly

with the base unit **112** without going through a repeater. It will also be understood by one of ordinary skill in the art that FIG. **1** shows only five sensor units (**102-106**) and two repeater units (**110-111**) for purposes of illustration and not by way of limitation. An installation in a large apartment building or complex would typically involve many sensor units and repeater units. Moreover, one of ordinary skill in the art will recognize that one repeater unit can service relatively many sensor units. In one embodiment, the sensor units **102** can communicate directly with the base unit **112** without going through a repeater **110**.

When the sensor unit **102** detects an anomalous condition (e.g., smoke, fire, water, etc.) the sensor unit communicates with the appropriate repeater unit **110** and provides data regarding the anomalous condition. The repeater unit **110** forwards the data to the base unit **112**, and the base unit **112** forwards the information to the computer **113**. The computer **113** evaluates the data and takes appropriate action. If the computer **113** determines that the condition is an emergency (e.g., fire, smoke, large quantities of water), then the computer **113** contacts the appropriate personnel **120**. If the computer **113** determines that the situation warrants reporting, but is not an emergency, then the computer **113** logs the data for later reporting. In this way, the sensor system **100** can monitor the conditions in and around the building **101**.

In one embodiment, the sensor unit **102** has an internal power source (e.g., battery, solar cell, fuel cell, etc.). In order to conserve power, the sensor unit **102** is normally placed in a low-power mode. In one embodiment, using sensors that require relatively little power, while in the low-power mode the sensor unit **102** takes regular sensor readings and evaluates the readings to determine if an anomalous condition exists. In one embodiment, using sensors that require relatively more power, while in the low-power mode, the sensor unit **102** takes and evaluates sensor readings at periodic intervals. If an anomalous condition is detected, then the sensor unit **102** "wakes up" and begins communicating with the base unit **112** through the repeater **110**. At programmed intervals, the sensor unit **102** also "wakes up" and sends status information (e.g., power levels, self diagnostic information, etc.) to the base unit (or repeater) and then listens for commands for a period of time. In one embodiment, the sensor unit **102** also includes a tamper detector. When tampering with the sensor unit **102** is detected, the sensor unit **102** reports such tampering to the base unit **112**.

In one embodiment, the sensor unit **102** provides bi-directional communication and is configured to receive data and/or instructions from the base unit **112**. Thus, for example, the base unit **112** can instruct the sensor unit **102** to perform additional measurements, to go to a standby mode, to wake up, to report battery status, to change wake-up interval, to run self-diagnostics and report results, etc. In one embodiment, the sensor unit **102** reports its general health and status on a regular basis (e.g., results of self-diagnostics, battery health, etc.)

In one embodiment, the sensor unit **102** provides two wake-up modes; a first wake-up mode for taking measurements (and reporting such measurements if deemed necessary), and a second wake-up mode for listening for commands from the central reporting station. The two wake-up modes, or combinations thereof, can occur at different intervals.

In one embodiment, the sensor unit **102** uses spread-spectrum techniques to communicate with the repeater unit **110**. In one embodiment, the sensor unit **102** uses frequency-hopping spread-spectrum. In one embodiment, the sensor unit **102** has an address or identification (ID) code that distinguishes the sensor unit **102** from the other sensor units. The sensor unit **102** attaches its ID to outgoing communication packets so that transmissions from the sensor unit **102** can be identified by the repeater **110**. The repeater **110** attaches the ID of the sensor unit **102** to data and/or instructions that are transmitted to the sensor unit **102**. In one embodiment, the sensor unit **102** ignores data and/or instructions that are addressed to other sensor units.

In one embodiment, the sensor unit **102** includes a reset function. In one embodiment, the reset function is activated by the reset switch **208**. In one embodiment, the reset function is active for a prescribed interval of time. During the reset interval, the transceiver **203** is in a receiving mode and can receive the identification code from an external programmer. In one embodiment, the external programmer wirelessly transmits a desired identification code. In one embodiment, the identification code is programmed by an external programmer that is connected to the sensor unit **102** through an electrical connector. In one embodiment, the electrical connection to the sensor unit **102** is provided by sending modulated control signals (power line carrier signals) through a connector used to connect the power source **206**. In one embodiment, the external programmer provides power and control signals. In one embodiment, the external programmer also programs the type of sensor(s) installed in the sensor unit. In one embodiment, the identification code includes an area code (e.g., apartment number, zone number, floor number, etc.) and a unit number (e.g., unit **1**, **2**, **3**, etc.).

In one embodiment, the sensor communicates with the repeater on the 900 MHz band. This band provides good transmission through walls and other obstacles normally found in and around a building structure. In one embodiment, the sensor communicates with the repeater on bands above and/or below the 900 MHz band. In one embodiment, the sensor, repeater, and/or base unit listen to a radio frequency channel before transmitting on that channel or before beginning transmission. If the channel is in use, (e.g., by another device such as, another repeater, a cordless telephone, etc.) then the sensor, repeater, and/or base unit changes to a different channel. In one embodiment, the sensor, repeater, and/or base unit coordinate frequency hopping by listening to radio frequency channels for interference and using an algorithm to select a next channel for transmission that avoids the interference. Thus, for example, in one embodiment, if a sensor senses a dangerous condition and goes into a continuous transmission mode, the sensor will test (e.g., listen to) the channel before transmission to avoid channels that are blocked, in use, or jammed. In one embodiment, the sensor continues to transmit data until it receives an acknowledgement from the base unit that the message has been received. In one embodiment, the sensor transmits data having a normal priority (e.g., status information) and does not look for an acknowledgement, and the sensor transmits data having elevated priority (e.g., excess smoke, temperature, etc.) until an acknowledgement is received.

The repeater unit **110** is configured to relay communications traffic between the sensor **102** (and, similarly, the sensor units **103-104**) and the base unit **112**. The repeater unit **110** typically operates in an environment with several other repeater units (such as the repeater unit **111** in FIG. **1**) and thus, the repeater unit **110** contains a database (e.g., a lookup table) of sensor unit IDs. In FIG. **1**, the repeater **110** has database entries for the Ids of the sensors **102-104**, and thus, the sensor **110** will only communicate with sensor units **102-104**. In one embodiment, the repeater **110** has an internal power source (e.g., battery, solar cell, fuel cell, etc.)

and conserves power by maintaining an internal schedule of when the sensor units **102-104** are expected to transmit. In one embodiment, the repeater unit **110** goes to a low-power mode when none of its designated sensor units is scheduled to transmit. In one embodiment, the repeater **110** uses spread-spectrum techniques to communicate with the base unit **112** and with the sensor units **102-104**. In one embodiment, the repeater **110** uses frequency-hopping spread-spectrum to communicate with the base unit **112** and the sensor units **102-104**. In one embodiment, the repeater unit **110** has an address or identification (ID) code and the repeater unit **110** attaches its address to outgoing communication packets that originate in the repeater (that is, packets that are not being forwarded). In one embodiment, the repeater unit **110** ignores data and/or instructions that are addressed to other repeater units or to sensor units not serviced by the repeater **110**.

In one embodiment, the base unit **112** communicates with the sensor unit **102** by transmitting a communication packet addressed to the sensor unit **102**. The repeaters **110** and **111** both receive the communication packet addressed to the sensor unit **102**. The repeater unit **111** ignores the communication packet addressed to the sensor unit **102**. The repeater unit **110** transmits the communication packet addressed to the sensor unit **102** to the sensor unit **102**. In one embodiment, the sensor unit **102**, the repeater unit **110**, and the base unit **112** communicate using Frequency-Hopping Spread Spectrum (FHSS), also known as channel-hopping.

Frequency-hopping wireless systems offer the advantage of avoiding other interfering signals and avoiding collisions. Moreover, there are regulatory advantages given to systems that do not transmit continuously at one frequency. Channel-hopping transmitters change frequencies after a period of continuous transmission, or when interference is encountered. These systems may have higher transmit power and relaxed limitations on in-band spurs. FCC regulations limit transmission time on one channel to 400 milliseconds (averaged over 10-20 seconds depending on channel bandwidth) before the transmitter must change frequency. There is a minimum frequency step when changing channels to resume transmission. If there are 25 to 49 frequency channels, regulations allow effective radiated power of 24 dBm, spurs must be −20 dBc, and harmonics must be −41.2 dBc. With 50 or more channels, regulations allow effective radiated power to be up to 30 dBm.

In one embodiment, the sensor unit **102**, the repeater unit **110**, and the base unit **112** communicate using FHSS wherein the frequency hopping of the sensor unit **102**, the repeater unit **110**, and the base unit **112** are not synchronized such that at any given moment, the sensor unit **102** and the repeater unit **110** are on different channels. In such a system, the base unit **112** communicates with the sensor unit **102** using the hop frequencies synchronized to the repeater unit **110** rather than the sensor unit **102**. The repeater unit **110** then forwards the data to the sensor unit using hop frequencies synchronized to the sensor unit **102**. Such a system largely avoids collisions between the transmissions by the base unit **112** and the repeater unit **110**.

In one embodiment, the sensor units **102-106** all use FHSS and the sensor units **102-106** are not synchronized. Thus, at any given moment, it is unlikely that any two or more of the sensor units **102-106** will transmit on the same frequency. In this manner, collisions are largely avoided. In one embodiment, collisions are not detected but are tolerated by the system **100**. If a collision does occur, data lost due to the collision is effectively re-transmitted the next time the sensor units transmit sensor data. When the sensor units **102-106** and repeater units **110-111** operate in asynchronous mode, then a second collision is highly unlikely because the units causing the collisions have hopped to different channels. In one embodiment, the sensor units **102-106**, repeater units **110-111**, and the base unit **112** use the same hop rate. In one embodiment, the sensor units **102-106**, repeater units **110-111**, and the base unit **112** use the same pseudo-random algorithm to control channel hopping, but with different starting seeds. In one embodiment, the starting seed for the hop algorithm is calculated from the ID of the sensor units **102-106**, repeater units **110-111**, or the base unit **112**.

In an alternative embodiment, the base unit communicates with the sensor unit **102** by sending a communication packet addressed to the repeater unit **112**, where the packet sent to the repeater unit **110** includes the address of the sensor unit **102**. The repeater unit **102** extracts the address of the sensor unit **102** from the packet and creates and transmits a packet addressed to the sensor unit **102**.

In one embodiment, the repeater unit **110** is configured to provide bi-directional communication between its sensors and the base unit **112**. In one embodiment, the repeater **110** is configured to receive instructions from the base unit **110**. Thus, for example, the base unit **112** can instruct the repeater to: send commands to one or more sensors; go to standby mode; "wake up"; report battery status; change wake-up interval; run self-diagnostics and report results; etc.

The base unit **112** is configured to receive measured sensor data from a number of sensor units either directly, or through the repeaters **110-111**. The base unit **112** also sends commands to the repeater units **110-111** and/or to the sensor units **102-106**. In one embodiment, the base unit **112** communicates with a diskless computer **113** that runs off of a CD-ROM. When the base unit **112** receives data from a sensor unit **102-106** indicating that there may be an emergency condition (e.g., a fire or excess smoke, temperature, water, etc.) the computer **113** will attempt to notify the responsible party **120**.

In one embodiment, the computer **112** maintains a database of the health, power status (e.g., battery charge), and current operating status of all of the sensor units **102-106** and the repeater units **110-111**. In one embodiment, the computer **113** automatically performs routine maintenance by sending commands to each sensor units **102-106** to run a self-diagnostic and report the results. The computer **113** collects and logs such diagnostic results. In one embodiment, the computer **113** sends instructions to each sensor units **102-106** telling the sensor how long to wait between "wakeup" intervals. In one embodiment, the computer **113** schedules different wakeup intervals to different sensor units **102-106** based on the sensor unit's health, power status, location, etc. In one embodiment, the computer **113** schedules different wakeup intervals to different sensor units **102-106** based on the type of data and urgency of the data collected by the sensor unit (e.g., sensor units that have smoke and/or temperature sensors produce data that should be checked relatively more often than sensor units that have humidity or moisture sensors). In one embodiment, the base unit sends instructions to repeaters to route sensor information around a failed repeater.

In one embodiment, the computer **113** produces a display that tells maintenance personnel which sensor units **102-106** need repair or maintenance. In one embodiment, the computer **113** maintains a list showing the status and/or location of each sensor according to the ID of each sensor.

In one embodiment, the sensor units **102-106** and/or the repeater units **110-111** measure the signal strength of the

wireless signals received (e.g., the sensor unit **102** measures the signal strength of the signals received from the repeater unit **110**, the repeater unit **110** measures the signal strength received from the sensor unit **102** and/or the base unit **112**). The sensor units **102-106** and/or the repeater units **110-111** report such signal strength measurement back to the computer **113**. The computer **113** evaluates the signal strength measurements to ascertain the health and robustness of the sensor system **100**. In one embodiment, the computer **113** uses the signal strength information to re-route wireless communications traffic in the sensor system **100**. Thus, for example, if the repeater unit **110** goes offline or is having difficulty communicating with the sensor unit **102**, the computer **113** can send instructions to the repeater unit **111** to add the ID of the sensor unit **102** to the database of the repeater unit **111** (and similarly, send instructions to the repeater unit **110** to remove the ID of the sensor unit **102**), thereby routing the traffic for the sensor unit **102** through the router unit **111** instead of the router unit **110**.

FIG. **2** is a block diagram of the sensor unit **102**. In the sensor unit **102**, one or more sensors **201** and a transceiver **203** are provided to a controller **202**. The controller **202** typically provides power, data, and control information to the sensor(s) **201** and the transceiver **203**. A power source **206** is provided to the controller **202**. An optional tamper sensor **205** is also provided to the controller **202**. A reset device (e.g., a switch) **208** is provided to the controller **202**. In one embodiment, an optional audio output device **209** is provided. In one embodiment, the sensor **201** is configured as a plug-in module that can be replaced relatively easily.

In one embodiment, the transceiver **203** is based on a TRF 6901 transceiver chip from Texas Instruments. Inc. In one embodiment, the controller **202** is a conventional programmable microcontroller. In one embodiment, the controller **202** is based on a Field Programmable Gate Array (FPGA), such as, for example, provided by Xilinx Corp. In one embodiment, the sensor **201** includes an optoelectric smoke sensor with a smoke chamber. In one embodiment, the sensor **201** includes a thermistor. In one embodiment, the sensor **201** includes a humidity sensor. In one embodiment, the sensor **201** includes a sensor, such as, for example, a water level sensor, a water temperature sensor, a carbon monoxide sensor, a moisture sensor, a water flow sensor, natural gas sensor, propane sensor, etc.

The controller **202** receives sensor data from the sensor(s) **201**. Some sensor(s) **201** produce digital data. However, for many types of sensor(s) **201**, the sensor data is analog data. Analog sensor data is converted to digital format by the controller **202**. In one embodiment, the controller evaluates the data received from the sensor(s) **201** and determines whether the data is to be transmitted to the base unit **112**. The sensor unit **102** generally conserves power by not transmitting data that falls within a normal range. In one embodiment, the controller **202** evaluates the sensor data by comparing the data value to a threshold value (e.g., a high threshold, a low threshold, or a high-low threshold). If the data is outside the threshold (e.g., above a high threshold, below a low threshold, outside an inner range threshold, or inside an outer range threshold), then the data is deemed to be anomalous and is transmitted to the base unit **112**. In one embodiment, the data threshold is programmed into the controller **202**. In one embodiment, the data threshold is programmed by the base unit **112** by sending instructions to the controller **202**. In one embodiment, the controller **202** obtains sensor data and transmits the data when commanded by the computer **113**.

In one embodiment, the tamper sensor **205** is configured as a switch that detects removal of/or tampering with the sensor unit **102**.

FIG. **3** is a block diagram of the repeater unit **110**. In the repeater unit **110**, a first transceiver **302** and a second transceiver **304** are provided to a controller **303**. The controller **303** typically provides power, data, and control information to the transceivers **302**, **304**. A power source **306** is provided to the controller **303**. An optional tamper sensor (not shown) is also provided to the controller **303**.

When relaying sensor data to the base unit **112**, the controller **303** receives data from the first transceiver **303** and provides the data to the second transceiver **304**. When relaying instructions from the base unit **112** to a sensor unit, the controller **303** receives data from the second transceiver **304** and provides the data to the first transceiver **302**. In one embodiment, the controller **303** conserves power by powering-down the transceivers **302**, **304** during periods when the controller **303** is not expecting data. The controller **303** also monitors the power source **306** and provides status information, such as, for example, self-diagnostic information and/or information about the health of the power source **306**, to the base unit **112**. In one embodiment, the controller **303** sends status information to the base unit **112** at regular intervals. In one embodiment, the controller **303** sends status information to the base unit **112** when requested by the base unit **112**. In one embodiment, the controller **303** sends status information to the base unit **112** when a fault condition (e.g., battery low) is detected.

In one embodiment, the controller **303** includes a table or list of identification codes for wireless sensor units **102**. The repeater **303** forwards packets received from, or sent to, sensor units **102** in the list. In one embodiment, the repeater **110** receives entries for the list of sensor units from the computer **113**. In one embodiment, the controller **303** determines when a transmission is expected from the sensor units **102** in the table of sensor units and places the repeater **110** (e.g., the transceivers **302**, **304**) in a low-power mode when no transmissions are expected from the transceivers on the list. In one embodiment, the controller **303** recalculates the times for low-power operation when a command to change reporting interval is forwarded to one of the sensor units **102** in the list (table) of sensor units or when a new sensor unit is added to the list (table) of sensor units.

FIG. **4** is a block diagram of the base unit **112**. In the base unit **112**, a transceiver **402** and a computer interface **404** are provided to a controller **403**. The controller **303** typically provides data and control information to the transceivers **402** and to the interface. The interface **404** is provided to a port on the monitoring computer **113**. The interface **404** can be a standard computer data interface, such as, for example, Ethernet, wireless Ethernet, firewire port, Universal Serial Bus (USB) port, bluetooth, etc.

FIG. **5** shows one embodiment of a communication packet **500** used by the sensor units, repeater units, and the base unit. The packet **500** includes a preamble portion **501**, an address (or ID) portion **502**, a data payload portion **503**, and an integrity portion **504**. In one embodiment, the integrity portion **504** includes a checksum. In one embodiment, the sensor units **102-106**, the repeater units **110-111**, and the base unit **112** communicate using packets such as the packet **500**. In one embodiment, the packets **500** are transmitted using FHSS.

In one embodiment, the data packets that travel between the sensor unit **102**, the repeater unit **111**, and the base unit **112** are encrypted. In one embodiment, the data packets that travel between the sensor unit **102**, the repeater unit **111**, and

the base unit **112** are encrypted and an authentication code is provided in the data packet so that the sensor unit **102**, the repeater unit, and/or the base unit **112** can verify the authenticity of the packet.

In one embodiment the address portion **502** includes a first code and a second code. In one embodiment, the repeater **111** only examines the first code to determine if the packet should be forwarded. Thus, for example, the first code can be interpreted as a building (or building complex) code and the second code interpreted as a subcode (e.g., an apartment code, area code, etc.). A repeater that uses the first code for forwarding, thus, forwards packets having a specified first code (e.g., corresponding to the repeater's building or building complex). Thus, alleviates the need to program a list of sensor units **102** into a repeater, since a group of sensors in a building will typically all have the same first code but different second codes. A repeater so configured, only needs to know the first code to forward packets for any repeater in the building or building complex. This does, however, raise the possibility that two repeaters in the same building could try to forward packets for the same sensor unit **102**. In one embodiment, each repeater waits for a programmed delay period before forwarding a packet. Thus reducing the chance of packet collisions at the base unit (in the case of sensor unit to base unit packets) and reducing the chance of packet collisions at the sensor unit (in the case of base unit to sensor unit packets). In one embodiment, a delay period is programmed into each repeater. In one embodiment, delay periods are pre-programmed onto the repeater units at the factory or during installation. In one embodiment, a delay period is programmed into each repeater by the base unit **112**. In one embodiment, a repeater randomly chooses a delay period. In one embodiment, a repeater randomly chooses a delay period for each forwarded packet. In one embodiment, the first code is at least 6 digits. In one embodiment, the second code is at least 5 digits.

In one embodiment, the first code and the second code are programmed into each sensor unit at the factory. In one embodiment, the first code and the second code are programmed when the sensor unit is installed. In one embodiment, the base unit **112** can re-program the first code and/or the second code in a sensor unit.

In one embodiment, collisions are further avoided by configuring each repeater unit **111** to begin transmission on a different frequency channel. Thus, if two repeaters attempt to begin transmission at the same time, the repeaters will not interfere with each other because the transmissions will begin on different channels (frequencies).

FIG. **6** is a flowchart showing one embodiment of the operation of the sensor unit **102** wherein relatively continuous monitoring is provided. In FIG. **6**, a power up block **601** is followed by an initialization block **602**. After initialization, the sensor unit **102** checks for a fault condition (e.g., activation of the tamper sensor, low battery, internal fault, etc.) in a block **603**. A decision block **604** checks the fault status. If a fault has occurred, then the process advances to a block **605** were the fault information is transmitted to the repeater **110** (after which, the process advances to a block **612**); otherwise, the process advances to a block **606**. In the block **606**, the sensor unit **102** takes a sensor reading from the sensor(s) **201**. The sensor data is subsequently evaluated in a block **607**. If the sensor data is abnormal, then the process advances to a transmit block **609** where the sensor data is transmitted to the repeater **110** (after which, the process advances to a block **612**); otherwise, the process advances to a timeout decision block **610**. If the timeout period has not elapsed, then the process returns to the fault-check block **603**; otherwise, the process advances to a transmit status block **611** where normal status information is transmitted to the repeater **110**. In one embodiment, the normal status information transmitted is analogous to a simple "ping" which indicates that the sensor unit **102** is functioning normally. After the block **611**, the process proceeds to a block **612** where the sensor unit **102** momentarily listens for instructions from the monitor computer **113**. If an instruction is received, then the sensor unit **102** performs the instructions, otherwise, the process returns to the status check block **603**. In one embodiment, transceiver **203** is normally powered down. The controller **202** powers up the transceiver **203** during execution of the blocks **605**, **609**, **611**, and **612**. The monitoring computer **113** can send instructions to the sensor unit **102** to change the parameters used to evaluate data used in block **607**, the listen period used in block **612**, etc.

Relatively continuous monitoring, such as shown in FIG. **6**, is appropriate for sensor units that sense relatively high-priority data (e.g., smoke, fire, carbon monoxide, flammable gas, etc.). By contrast, periodic monitoring can be used for sensors that sense relatively lower priority data (e.g., humidity, moisture, water usage, etc.). FIG. **7** is a flowchart showing one embodiment of operation of the sensor unit **102** wherein periodic monitoring is provided. In FIG. **7**, a power up block **701** is followed by an initialization block **702**. After initialization, the sensor unit **102** enters a low-power sleep mode. If a fault occurs during the sleep mode (e.g., the tamper sensor is activated), then the process enters a wake-up block **704** followed by a transmit fault block **705**. If no fault occurs during the sleep period, then when the specified sleep period has expired, the process enters a block **706** where the sensor unit **102** takes a sensor reading from the sensor(s) **201**. The sensor data is subsequently sent to the monitoring computer **113** in a report block **707**. After reporting, the sensor unit **102** enters a listen block **708** where the sensor unit **102** listens for a relatively short period of time for instructions from monitoring computer **708**. If an instruction is received, then the sensor unit **102** performs the instructions, otherwise, the process returns to the sleep block **703**. In one embodiment, the sensor **201** and transceiver **203** are normally powered down. The controller **202** powers up the sensor **201** during execution of the block **706**. The controller **202** powers up the transceiver during execution of the blocks **705**, **707**, and **708**. The monitoring computer **113** can send instructions to the sensor unit **102** to change the sleep period used in block **703**, the listen period used in block **708**, etc.

In one embodiment, the sensor unit transmits sensor data until a handshaking-type acknowledgement is received. Thus, rather than sleep of no instructions or acknowledgements are received after transmission (e.g., after the decision block **613** or **709**) the sensor unit **102** retransmits its data and waits for an acknowledgement. The sensor unit **102** continues to transmit data and wait for an acknowledgement until an acknowledgement is received. In one embodiment, the sensor unit accepts an acknowledgement from a repeater unit **111** and it then becomes the responsibility of the repeater unit **111** to make sure that the data is forwarded to the base unit **112**. In one embodiment, the repeater unit **111** does not generate the acknowledgement, but rather forwards an acknowledgement from the base unit **112** to the sensor unit **102**. The two-way communication ability of the sensor unit **102** provides the capability for the base unit **112** to control the operation of the sensor unit **102** and also provides the capability for robust handshaking-type communication between the sensor unit **102** and the base unit **112**.

Regardless of the normal operating mode of the sensor unit **102** (e.g., using the Flowcharts of FIGS. **6**, **7**, or other modes) in one embodiment, the monitoring computer **113** can instruct the sensor unit **102** to operate in a relatively continuous mode where the sensor repeatedly takes sensor readings and transmits the readings to the monitoring computer **113**. Such a mode would can be used, for example, when the sensor unit **102** (or a nearby sensor unit) has detected a potentially dangerous condition (e.g., smoke, rapid temperature rise, etc.)

FIG. **8** shows the sensor system used to detect water leaks. In one embodiment, the sensor unit **102** includes a water level sensor **803** and/or a water temperature sensor **804**. The water level sensor **803** and/or water temperature sensor **804** are placed, for example, in a tray underneath a water heater **801** in order to detect leaks from the water heater **801** and, thereby, prevent water damage from a leaking water heater. In one embodiment, a temperature sensor is also provided to measure temperature near the water heater. The water level sensor can also be placed under a sink, in a floor sump, etc. In one embodiment, the severity of a leak is ascertained by the sensor unit **102** (or the monitoring computer **113**) by measuring the rate of rise in the water level. When placed near the hot water tank **801**, the severity of a leak can also be ascertained at least in part by measuring the temperature of the water. In one embodiment, a first water flow sensor is placed in an input water line for the hot water tank **801** and a second water flow sensor is placed in an output water line for the hot water tank. Leaks in the tank can be detected by observing a difference between the water flowing through the two sensors.

In one embodiment, a remote shutoff valve **810** is provided, so that the monitoring system **100** can shutoff the water supply to the water heater when a leak is detected. In one embodiment, the shutoff valve is controlled by the sensor unit **102**. In one embodiment, the sensor unit **102** receives instructions from the base unit **112** to shut off the water supply to the heater **801**. In one embodiment, the responsible party **120** sends instructions to the monitoring computer **113** instructing the monitoring computer **113** to send water shut off instructions to the sensor unit **102**. Similarly, in one embodiment, the sensor unit **102** controls a gas shutoff valve **811** to shut off the gas supply to the water heater **801** and/or to a furnace (not shown) when dangerous conditions (such as, for example, gas leaks, carbon monoxide, etc.) are detected. In one embodiment, a gas detector **812** is provided to the sensor unit **102**. In one embodiment, the gas detector **812** measures carbon monoxide. In one embodiment, the gas detector **812** measures flammable gas, such as, for example, natural gas or propane.

In one embodiment, an optional temperature sensor **818** is provided to measure stack temperature. Using data from the temperature sensor **818**, the sensor unit **102** reports conditions, such as, for example, excess stack temperature. Excess stack temperature is often indicative of poor heat transfer (and thus, poor efficiency) in the water heater **801**.

In one embodiment, an optional temperature sensor **818** is provided to measure temperature of water in the water heater **801**. Using data from the temperature sensor **819**, the sensor unit **102** reports conditions, such as, for example, over-temperature or under-temperature of the water in the water heater.

In one embodiment, an optional current probe **821** is provided to measure electric current provided to a heating element **820** in an electric water heater. Using data from the current probe **821**, the sensor unit **102** reports conditions, such as, for example, no current (indicating a burned-out heating element **820**). An over-current condition often indicates that the heating element **820** is encrusted with mineral deposits and needs to be replaced or cleaned. By measuring the current provided to the water heater, the monitoring system can measure the amount of energy provided to the water heater and thus the cost of hot water, and the efficiency of the water heater.

In one embodiment, the sensor **803** includes a moisture sensor. Using data from the moisture sensor, the sensor unit **102** reports moisture conditions, such as, for example, excess moisture that would indicate a water leak, excess condensation, etc.

In one embodiment, the sensor unit **102** is provided to a moisture sensor (such as the sensor **803**) located near an air conditioning unit. Using data from the moisture sensor, the sensor unit **102** reports moisture conditions, such as, for example, excess moisture that would indicate a water leak, excess condensation, etc.

In one embodiment, the sensor **201** includes a moisture sensor. The moisture sensor can be place under a sink or a toilet (to detect plumbing leaks) or in an attic space (to detect roof leaks).

Excess humidity in a structure can cause severe problems such as rotting, growth of molds, mildew, and fungus, etc. (hereinafter referred to generically as fungus). In one embodiment, the sensor **201** includes a humidity sensor. The humidity sensor can be placed under a sink, in an attic space, etc., to detect excess humidity (due to leaks, condensation, etc.). In one embodiment, the monitoring computer **113** compares humidity measurements taken from different sensor units in order to detect areas that have excess humidity. Thus, for example, the monitoring computer **113** can compare the humidity readings from a first sensor unit **102** in a first attic area, to a humidity reading from a second sensor unit **102** in a second area. For example, the monitoring computer can take humidity readings from a number of attic areas to establish a baseline humidity reading and then compare the specific humidity readings from various sensor units to determine if one or more of the units are measuring excess humidity. The monitoring computer **113** would flag areas of excess humidity for further investigation by maintenance personnel. In one embodiment, the monitoring computer **113** maintains a history of humidity readings for various sensor units and flags areas that show an unexpected increase in humidity for investigation by maintenance personnel.

In one embodiment, the monitoring system **100** detects conditions favorable for fungus (e.g., mold, mildew, fungus, etc.) growth by using a first humidity sensor located in a first building area to produce first humidity data and a second humidity sensor located in a second building area to produce second humidity data. The building areas can be, for example, areas near a sink drain, plumbing fixture, plumbing, attic areas, outer walls, a bilge area in a boat, etc.

The monitoring station **113** collects humidity readings from the first humidity sensor and the second humidity sensor and indicates conditions favorable for fungus growth by comparing the first humidity data and the second humidity data. In one embodiment, the monitoring station **113** establishes a baseline humidity by comparing humidity readings from a plurality of humidity sensors and indicates possible fungus growth conditions in the first building area when at least a portion of the first humidity data exceeds the baseline humidity by a specified amount. In one embodiment, the monitoring station **113** establishes a baseline humidity by comparing humidity readings from a plurality of humidity sensors and indicates possible fungus growth

conditions in the first building area when at least a portion of the first humidity data exceeds the baseline humidity by a specified percentage.

In one embodiment, the monitoring station **113** establishes a baseline humidity history by comparing humidity readings from a plurality of humidity sensors and indicates possible fungus growth conditions in the first building area when at least a portion of the first humidity data exceeds the baseline humidity history by a specified amount over a specified period of time. In one embodiment, the monitoring station **113** establishes a baseline humidity history by comparing humidity readings from a plurality of humidity sensors over a period of time and indicates possible fungus growth conditions in the first building area when at least a portion of the first humidity data exceeds the baseline humidity by a specified percentage of a specified period of time.

In one embodiment, the sensor unit **102** transmits humidity data when it determines that the humidity data fails a threshold test. In one embodiment, the humidity threshold for the threshold test is provided to the sensor unit **102** by the monitoring station **113**. In one embodiment, the humidity threshold for the threshold test is computed by the monitoring station from a baseline humidity established in the monitoring station. In one embodiment, the baseline humidity is computed at least in part as an average of humidity readings from a number of humidity sensors. In one embodiment, the baseline humidity is computed at least in part as a time average of humidity readings from a number of humidity sensors. In one embodiment, the baseline humidity is computed at least in part as a time average of humidity readings from a humidity sensor. In one embodiment, the baseline humidity is computed at least in part as the lesser of a maximum humidity reading an average of a number of humidity readings.

In one embodiment, the sensor unit **102** reports humidity readings in response to a query by the monitoring station **113**. In one embodiment, the sensor unit **102** reports humidity readings at regular intervals. In one embodiment, a humidity interval is provided to the sensor unit **102** by the monitoring station **113**.

In one embodiment, the calculation of conditions for fungus growth is comparing humidity readings from one or more humidity sensors to the baseline (or reference) humidity. In one embodiment, the comparison is based on comparing the humidity readings to a percentage (e.g., typically a percentage greater than 100%) of the baseline value. In one embodiment, the comparison is based on comparing the humidity readings to a specified delta value above the reference humidity. In one embodiment, the calculation of likelihood of conditions for fungus growth is based on a time history of humidity readings, such that the longer the favorable conditions exist, the greater the likelihood of fungus growth. In one embodiment, relatively high humidity readings over a period of time indicate a higher likelihood of fungus growth than relatively high humidity readings for short periods of time. In one embodiment, a relatively sudden increase in humidity as compared to a baseline or reference humidity is reported by the monitoring station **113** as a possibility of a water leak. If the relatively high humidity reading continues over time then the relatively high humidity is reported by the monitoring station **113** as possibly being a water leak and/or an area likely to have fungus growth or water damage.

Temperatures relatively more favorable to fungus growth increase the likelihood of fungus growth. In one embodiment, temperature measurements from the building areas are also used in the fungus grown-likelihood calculations. In one embodiment, a threshold value for likelihood of fungus growth is computed at least in part as a function of temperature, such that temperatures relatively more favorable to fungus growth result in a relatively lower threshold than temperatures relatively less favorable for fungus growth. In one embodiment, the calculation of a likelihood of fungus growth depends at least in part on temperature such that temperatures relatively more favorable to fungus growth indicate a relatively higher likelihood of fungus growth than temperatures relatively less favorable for fungus growth. Thus, in one embodiment, a maximum humidity and/or minimum threshold above a reference humidity is relatively lower for temperature more favorable to fungus growth than the maximum humidity and/or minimum threshold above a reference humidity for temperatures relatively less favorable to fungus growth.

In one embodiment, a water flow sensor is provided to the sensor unit **102**. The sensor unit **102** obtains water flow data from the water flow sensor and provides the water flow data to the monitoring computer **113**. The monitoring computer **113** can then calculate water usage. Additionally, the monitoring computer can watch for water leaks, by, for example, looking for water flow when there should be little or no flow. Thus, for example, if the monitoring computer detects water usage throughout the night, the monitoring computer can raise an alert indicating that a possible water leak has occurred.

In one embodiment, the sensor **201** includes a water flow sensor is provided to the sensor unit **102**. The sensor unit **102** obtains water flow data from the water flow sensor and provides the water flow data to the monitoring computer **113**. The monitoring computer **113** can then calculate water usage. Additionally, the monitoring computer can watch for water leaks, by, for example, looking for water flow when there should be little or no flow. Thus, for example, if the monitoring computer detects water usage throughout the night, the monitoring computer can raise an alert indicating that a possible water leak has occurred.

In one embodiment, the sensor **201**, which includes a fire-extinguisher tamper sensor, is provided to the sensor unit **102**. The fire-extinguisher tamper sensor reports tampering with or use of a fire-extinguisher. In one embodiment the fire-extinguisher temper sensor reports that the fire extinguisher has been removed from its mounting, that a fire extinguisher compartment has been opened, and/or that a safety lock on the fire extinguisher has been removed.

FIG. **9** is a flowchart **900** showing one embodiment for configuring the sensor system by labeling sensor units according to an intended location and providing computer data to correlate a sensor identification code with a sensor location. The flowchart **900** begins with a process block **901** wherein a user or other person specifying a sensor system produces a list of sensor locations including location data for each sensor. For example, the location data can specify the type of sensor (smoke, water, gas, etc.) and the location of the sensor. The location data for the sensor can be specified by apartment number, location in an apartment (e.g., kitchen, hallway, bedroom, etc.). The location data can also specify the building (e.g., by address, building number, etc.) and/or floor number. In an industrial application, the location data can also specify the location of the sensor by type, location (e.g., building, building area, etc.), and the like. In one embodiment, portions of the process block **901** are performed by using the Internet. In one embodiment, the user or person specifying the system uses a World Wide Web (web) browser (e.g., Microsoft Internet Explorer, Mozilla,

Firefox, etc.) to visit a website that provides for ordering the sensor system. The user or person specifying the system uses the web browser to input the list of sensor locations and, optionally, to specify the sensor type at each location. Optionally, the user can also specify the number of repeaters and which sensors are served by each repeater.

The process then advances to a process block **902** where the location data is provided to a programming facility (e.g., a manufacturing facility, sales or distribution facility, on-site programming facility, etc.). The process then advances to a process block **903** where the programming facility produces a list of sensor ID's corresponding to the sensor locations. Thus, an sensor identification code is provided for each sensor at each specified location. The process then advances to a process block **904** where the list of sensor locations and corresponding sensor identification codes is stored as system configuration data for later recall. The process then advances to a process block **905** where each sensor is labeled. In one embodiment, each sensor is labeled according to its intended location so that an installer can easily identify where each sensor is to be placed. In one embodiment, the sensor label includes the identification code. In one embodiment, the sensor label includes a bar code. In one embodiment, the sensor label includes the sensor type. The process then advances to a process block **906** wherein the labeled sensor units and a computer-readable media or network location containing the system configuration data are provided to the user. The system configuration data includes the list of sensor locations and corresponding sensor identification codes. The computer-readable media (or network location can be provided to the control system **113** to configure the sensor system so that the control system **113** knows which sensors are installed, their identification numbers, and locations. Thus, the control system **113** knows which sensors to monitor and where to report sensor locations when a sensor reports an anomalous condition.

FIG. **10** is a flowchart **1000** for one embodiment for adding sensors to an existing system. The flowchart **1000** begins with a process block **1001** wherein a user or other person specifying a sensor system produces produce a list of additional sensor locations including location data for each additional sensor unit to be added to the system. In one embodiment, portions of the process block **1001** are performed by using the Internet. In one embodiment, the user or person specifying the system uses a web browser to input the list of additional sensor locations and, optionally, to specify the sensor type at each location. Optionally, the user can also specify the number of repeaters and which sensors are served by each repeater.

The process then advances to a process block **1002** where the location data is provided to a programming facility (e.g., a manufacturing facility, sales or distribution facility, on-site programming facility, etc.). The process then advances to a process block **1003** where the programming facility retrieve the stored list of sensor locations and identification codes for the sensor system. The process then advances to process blocks **1004** and **1005**, where the programming facility adds sensor ID's and location data corresponding to the new sensor locations to the list of sensor location are added to the system configuration data and stored. The process then advances to a process block where the list of sensor identification codes and sensor locations (including the data for the new sensors) is stored. The process then advances to a process block **1007** where the new sensors a labeled with location information (and optionally identification information and/or barcode information). The process then advances to a process block **1008** where the new labeled sensor units and a computer-readable copy of the list of the system configuration data is provided to the user.

It will be evident to those skilled in the art that the invention is not limited to the details of the foregoing illustrated embodiments and that the present invention may be embodied in other specific forms without departing from the spirit or essential attributed thereof; furthermore, various omissions, substitutions and changes may be made without departing from the spirit of the inventions. For example, although specific embodiments are described in terms of the 900 MHz frequency band, one of ordinary skill in the art will recognize that frequency bands above and below 900 MHz can be used as well. The wireless system can be configured to operate on one or more frequency bands, such as, for example, the HF band, the VHF band, the UHF band, the Microwave band, the Millimeter wave band, etc. One of ordinary skill in the art will further recognize that techniques other than spread spectrum can also be used and/or can be used instead of spread spectrum. The modulation uses is not limited to any particular modulation method, such that modulation scheme used can be, for example, frequency modulation, phase modulation, amplitude modulation, combinations thereof, etc. The foregoing description of the embodiments is, therefore, to be considered in all respects as illustrative and not restrictive, with the scope of the invention being delineated by the appended claims and their equivalents.

What is claimed is:

1. A wireless sensor system, comprising:

a plurality of wireless sensor units, each of said one or more wireless sensor units comprising at least one sensor configured to measure a condition, said wireless sensor unit configured to receive instructions; each of said one or more wireless sensor units configured to report data measured by said at least one sensor when said wireless sensor determines that data measured by said at least one sensor fails a threshold test, each of said one or more sensor units provided with a label indicating an intended location for installation;

a computer-readable media provided with said one or more wireless sensor units, said computer-readable media containing data indicating said intended locations and corresponding identification codes for each of said sensor units; and

a base unit configured to communicate with said one or more wireless sensor units and to provide data from said one or more wireless sensor units to a monitoring computer, said monitoring computer configured to send a notification to a responsible party when data from one or more of said wireless sensor units corresponds to an emergency condition, said monitoring computer configured to log data from one or more of said wireless sensor units when said data from one or more of said wireless sensor units corresponds to an abnormal condition said monitoring computer configured to use data from said computer-readable medium to correlate said intended locations with said identification codes.

2. The wireless sensor system of claim **1**, wherein said at least one sensor comprises a smoke sensor.

3. The wireless sensor system of claim **1**, wherein said at least one sensor comprises an air temperature sensor.

4. The wireless sensor system of claim **1**, wherein said at least one sensor comprises a water-level sensor.

5. The wireless sensor system of claim **1**, wherein said at least one sensor comprises a water-temperature sensor.

6. The wireless sensor system of claim **1**, wherein said at least one sensor comprises a moisture sensor.

7. The wireless sensor system of claim 1, wherein said at least one sensor comprises a humidity sensor.

8. The wireless sensor system of claim 1, wherein said at least one sensor comprises a carbon monoxide sensor.

9. The wireless sensor system of claim 1, wherein said at least one sensor comprises a flammable gas sensor.

10. The wireless sensor system of claim 1, wherein said at least one sensor comprises a door-open sensor.

11. The wireless sensor system of claim 1, wherein said at least one sensor comprises a broken-window sensor.

12. The wireless sensor system of claim 1, wherein said at least one sensor comprises an intrusion sensor.

13. The wireless sensor system of claim 1, wherein said at least one sensor comprises a power-failure sensor.

14. The wireless sensor system of claim 1, wherein said monitoring computer is configured to attempt to contact said responsible party by telephone.

15. The wireless sensor system of claim 1, wherein said monitoring computer is configured to attempt to contact said responsible party by cellular telephone.

16. The wireless sensor system of claim 1, wherein said monitoring computer is configured to attempt to contact said responsible party by cellular text messaging.

17. The wireless sensor system of claim 1, wherein said monitoring computer is configured to attempt to contact said responsible party by pager.

18. The wireless sensor system of claim 1, wherein said monitoring computer is configured to attempt to contact said responsible party by Internet.

19. The wireless sensor system of claim 1, wherein said monitoring computer is configured to attempt to contact said responsible party by email.

20. The wireless sensor system of claim 1, wherein said monitoring computer is configured to attempt to contact said responsible party by Internet instant messaging.

21. The wireless sensor system of claim 1, wherein said monitoring computer comprises a diskless computer.

22. The wireless sensor system of claim 1, wherein said threshold test comprises a high threshold level.

23. The wireless sensor system of claim 1, wherein said threshold test comprises a low threshold level.

24. The wireless sensor system of claim 1, wherein said threshold test comprises an inner threshold range.

25. The wireless sensor system of claim 1, wherein said threshold test comprises an outer threshold range.

26. The wireless sensor system of claim 1, wherein said one or more wireless sensor units comprises a tamper sensor and an ambient condition sensor.

27. The wireless sensor system of claim 1, wherein said one or more wireless sensor units are configured to receive an instruction to change a status reporting interval.

28. The wireless sensor system of claim 1, wherein said one or more wireless sensor units are configured to receive an instruction to change a sensor data reporting interval.

29. The wireless sensor system of claim 1, wherein said monitoring computer is configured to monitor status of each of said one or more wireless sensors.

30. A method of configuring a sensor system, comprising:

generating a list of intended sensor unit locations including a first location and a second location;

programming a first sensor unit with a first identification code;

marking said first sensor unit with a first marking indicating said first location;

programming a second sensor unit with a second identification code;

marking said second sensor unit with a second marking indicating said second location;

writing a computer readable medium with data correlating said first marking with said first identification code and correlating said second marking with said second identification code; and

providing said first sensor unit and said second sensor unit and said computer readable medium to a user.

* * * * *