PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G08B 29/00, H04L 9/00

A1

(11) International Publication Number: **WO 96/33478**

(43) International Publication Date: 24 October 1996 (24.10.96)

(21) International Application Number: PCT/US95/04731

(22) International Filing Date: 17 April 1995 (17.04.95)

(71)(72) Applicant and Inventor: SANDERFORD, Hugh, Britton, Jr. [US/US]; Sanconix, Inc., Suite 202, 101 W. Robert E. Lee Boulevard, New Orleans, LA 70124 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: SOUVESTRE, John [US/US]; Suite 113, 3500 Houma Boulevard, Metairie, LA 70006 (US). REED, Marc [US/US]; 515 Nashville Avenue, New Orleans, LA 70115 (US).

(74) Agent: REGARD, Joseph, T.; Joseph T. Regard, Ltd. plc, Suite 100, 3200 Ridgelake Avenue, Metairie, LA 70002 (US).

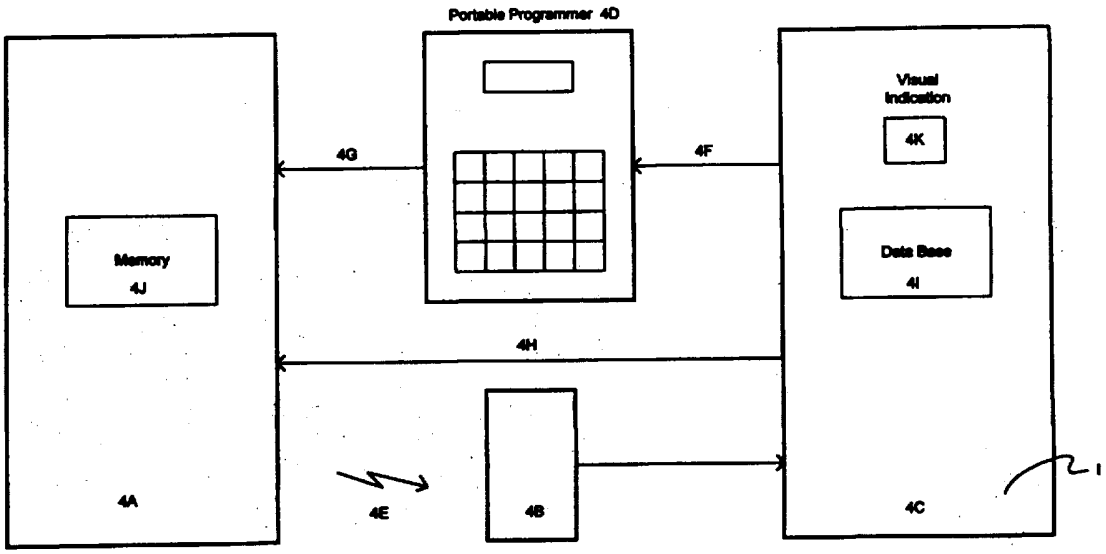
(81) Designated States: AU, CA, JP, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published

With international search report.

With amended claims.

(54) Title: SECURE REMOTE SENSOR/TRANSMITTER ARRAY SYSTEM



(57) Abstract

A system for preventing unauthorized access to the programming and control features of remote sensor transmitters (4A) utilized in a remote sensor/transmitter array, such as, for example, fire and/or security systems (4C) or the like. The exemplary embodiment of the present invention utilizes an association of transmitter identity/address with a central processor/control fire/security data base (4I) which in turn is configured to securely program each transmitter with its location and function, or "personality". Still other teachings of the present invention relate to a sensor transmitter (4A) which is shipped in a power saving mode, and which powers up upon sensing predetermined conditions, said sensor further including power saving transmission modes, EEROM power saving modes and redundant memory with error checking features, optical and magnetic loop power/programming systems, and a unique sequence of events "wake up" string.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

Title: Secure Remote Sensor/Transmitter Array System

Background of the Invention

Invention Field

The present invention relates to remote monitoring, including for example, remote sensor/transmission arrays including security/fire/alarm systems and the like, and more particularly to a system for preventing unauthorized access to the programming and control features of a remote sensors utilized in such a system. The exemplary embodiment of the present invention utilizes an association of transmitter identity/address with a central processor, or control panel/security data base, which in turn is configured to securely program each transmitter with its location and function, or "personality".

An alternative embodiment of the present invention teaches the utilization of a site- specific or customer specific seed incorporated into sensor/transmitter transmissions, in order to provide a secure means of communicating between the sensor and central processor/control panel. This secure programming may be accomplished utilizing an magnetic loop or other transmission means. Further, the present system contemplates the utilization of verification means to verify correct sensor programming, as well as a method of preventing alteration of sensor programming after installation via a JAM command.

The various, individual sensors and central processor/control unit communicate individually via individual, repeatable pseudo randomization algorithms, producing a several bit result. The communicating central processor/control and each sensor must have a match on outgoing/incoming code before the transmitting sensor will accept the programming on its personality. The exemplary embodiment of the present invention also utilizes a randomization seed, which can altered occasionally, to further increase security.

Still other teachings of the present invention relate to a sensor transmitter which is shipped in a power saving mode, and which powers up upon sensing predetermined conditions, said sensor further including power saving transmission modes, EEROM power saving modes and redundant memory with error checking features, optical and magnetic loop power/programming systems, and a unique sequence of events "wake up" string.

General Background Discussion

Most security systems configured for monitoring a perimeter utilize a plurality of individually programmed, remote sensors along said perimeter, with each of said sensors configured to communicate with a central processor/control unit via electromagnetic or optical link or the like. A recognized problem with such system rests with the integrity of the remote sensors, as alteration of their program can be utilized as a method of violating security.

A list of prior patents which may be of interest is presented below:

Patent No.	Patentee(s)	Issue Date
4,855,713	Brunius	08/08/1989
4,581,606	Mallory	03/08/1986

The '713 patent to Brunis teaches a "Learn Mode Transmitter", teaching a security system whereby a central processing unit self learns the identities of its distributed transmitter sensors, each of said transmitters containing signal conditioning data and a pseudo randomly programmed identity code.

The '713 patent, however, requires that each transmitter be pre-programmed at the factory, which further requires the utilization of additional non-volatile ram or burned-in PROM, which is not required by the present invention. Further if standard, volatile RAM is utilized in lieu of the above, the transmitter must be powered from its time of programming at the factory, via battery and any interruption in power due to burn out of the power supply or battery will result in loss of programming data, and the need for re-programming.

Further, it is believed that the '713 system requires extra modes in order to prevent the transmitters from continually transmitting while in shipment, not only to conserve batteries, but also to prevent dangerous conditions such transmissions may cause when in close proximity or aboard airplanes and the like. Such systems, if not deactivated in transport, have been known to cause false alarms in the security systems of the storage facility, etc.

In addition, if the pre-programmed transmitter of the '713 system were found to be in conflict with an existing programmed address after installation, it must be removed from the system and returned, as the address is fixed, unlike the present invention, as will be further discussed infra.

The '606 patent to Mallory teaches a "Central Monitor for Home Security System" wherein there is taught a system wherein each of the transmitters is programmed with individual information data, which is fed back to the central monitor during an alarm, which is matched with the data in the central monitor's memory for a match, which establishes the monitor and nature of the alarm.

However, the '606 device can be programmed by any unsecured, unauthorized programming device, since no scrambling or authorized identification mode is required; nor does said system contemplate a means to alter access codes for programming of transmitters.

Further, the '606 device requires the utilization of a programming wire which can easily be compromised (unlike the present invention), and which may not be removable when transmitters require magnetic, electromagnetic, or optical means of communication.

There is no JAM command provided with the Mallory device, so a similar programming device to that originally utilized in setting up the system may be later reconnected by an unauthorized user in reprogramming the system, compromising security.

Further, since there is no JAM command provided, the only way for the transmitter to achieve the secure mode of operation against future re-programming is the enclose the electrical programming pins in a secure housing with the addition of a tamper warning sensor, which then transmits the appropriate message, requiring additional hardware, software, and costs, and still do not provide absolute security.

This method would also not work in conjunction with a system relying upon non-wire transmission such as magnetic, electromagnetic, or optical transmitter programming means, as it would be impossible to "disconnect" such means fully, and transmission of same for unauthorized programming could occur at a great distance.

Lastly, Mallory has no provision of verifying the data being transferred to the transmitter, either by conversion of scrambling bits or via the re-transmission of programmed information.

Summary Discussion of the Invention

The present invention overcomes these prior art problems by providing a system wherein there is provided an association of transmitter identity/addresses with the central monitoring panel, which in turn is configured to securely program each transmitter with its location and function, or "personality"

The present invention is typically utilized with an array of remote sensor/transmitters, as utilized with, for example fire/security/control systems, which includes a central monitoring panel interfacing with a plurality of external sensors. The sensors may be configured to provide a wide variety of information in the form of monitoring for smoke, temperature flux, motion or heat detection, intrusion, water flow detection or monitoring, voice dispatch, voltage level monitoring, power meter monitoring, analog level reporting, or the like. Other applications may further include time and attendance accounting, building or home automation, process control, remote terminal programming, and the like.

Each of the above receivers in the present embodiment of the invention communicates via wire, radio, or optically with one or more receivers, relaying said information to the fire/security panel, which has the capacity to process said information according to the program, and act upon said information in the appropriate manner.

Each of said sensors must be set up with PERSONALITY information, assigning an identity of the unit amongst the other components in the system, as well as a function, appropriate response, and communication parameters and protocol, including identification/address bits, property/system code(s), frequency channel or spread spectrum channel, transmission timing, as well as input condition(s) and calibration.

An alternative embodiment of the present invention teaches the utilization of a site- specific or customer specific seed incorporated into sensor/transmitter transmissions, in order to provide a secure means of communicating between the sensor and central processor/control panel. This secure programming may be accomplished utilizing an magnetic loop or other transmission means. Further, the present system contemplates the utilization of verification means to verify correct sensor programming, as well as a method of preventing alteration of sensor programming after installation via a JAM command.

Still other teachings of the present invention relate to a sensor transmitter which is shipped in a power saving mode, and which powers up upon sensing predetermined conditions, said sensor further including power saving transmission modes, power backup mode, EEROM power saving modes and redundant memory with error checking features, optical and magnetic loop power/programming systems,

and a unique sequence of events "wake up" string.

It is essential that this initial programming of personality information be accurate and secure, as unauthorized future alteration of same thereafter can be utilized as a means of violating system integrity. The present invention discloses a system for insuring data security, and for preventing unauthorized alteration of the personality program of the sensors, once installed and set.

It is thus an object of the present invention to provide a system for the secure initial programming of sensory nodes in the sensory array of a monitoring/access/fire/security/control system.

It is another object of the present invention to provide a system for securely setting up and communicating with programmable remote components of various data arrays.

It is yet another object of the present invention to provide a system for securing individual sensory nodes in a sensory/transmitter and central processor/receiver arrangement.

It is another object of the present invention to provide a sensor transmitter which maybe programmed via limited field strength means such as magnetic loop coils, optical programming, or the like.

It is still another object of the present invention to provide a sensor transmitter which may utilize the magnetic field from an inductive transmitter such as a magnetic loop coil or the like for power during the programming phase.

It is still another object of the present invention to provide a sensor which remains in a energy conservation mode during storage, and is selectively initiated into a programming mode, during which time a sequence of programmed events occurs, including power up, handshaking with the programmer, initialize the programming mode, verification burst, jam command, and other features as desired.

BRIEF DESCRIPTION of the DRAWINGS

For a further understanding of the nature and objects of the present invention, reference should be had to the following detailed description, taken in conjunction with the accompanying drawings, in which like parts are given like reference numerals, and wherein:

Figure 1 is a logic circuit diagram of the sensor/transmitter programming input schematic of the preferred embodiment of the secure sensor/transmitter array of the present invention.

Figure 2 is a logic circuit of the jam command logic circuit schematic of the secure sensor/transmitter array of **Figure 1**.

Figure 3 is a diagram of the programming input schematic of the secure sensor/transmitter array of **Figure 1**.

Figure 4 is a block diagram of the system of programming the sensor/transmitter(s) comprising the secure sensor/transmitter array of **Figure 1**.

Figure 5 is a block diagram of the jam command and security/randomization bits of the secure sensor/transmitter array of **Figure 1**.

Figures 6a and **6b** illustrate an alternative embodiment of the present invention, which utilizes

EEROM in providing a power saving and redundant memory feature.

DETAILED DESCRIPTION of the INVENTION

The present invention teaches various and diverse improvements in the programming and operation of a sensor transmitter array in combination with a central processing unit, which may be in the form of a fire/security control panel. Amoung these is an association of transmitter identity/address with a fire/security panel data base, or central processing unit, which in turn contains transmitter location and function, typically for a plurality of individual transmitters forming a monitoring sensor array. The goals of such a process are as follows:

1. The process must be simple to perform in any field/installation related work.
2. The process must be economical and readily manufacturable.
3. The programming process and the resulting transmitter to panel association must be secure.
4. The process must not be able to be accomplished by an unauthorized person.
5. The process must not be able to be compromised once the transmitter to panel association is made.

By way of these methods, the fire/security panel, or other programming device, causes each sensor or TRANSMITTER to be programmed. The transmitters may be manufactured with NO or little initial "personality" or address/identification built in, although sensors may be set, as desired, at the factory with preliminary address and related information, and placed into a non-transmission mode for shipping, thereby providing a partial programming of the sensor.

After a transmitter is assembled, and before it can be placed in an operational environment, it must be tested. Generally, it is tested initially at the factory, as part of the manufacturing process. It is also tested after installation. At times, it may also be desirable to run certain tests, either in the lab or in the field. All of these tests are greatly facilitated by the inclusion of certain "test modes", in the transmitters firmware. For example, "fast transmit", and "continuous transmit", although power intensive, are desirable during manufacturing, as they can allow the sensor transmitters to provide regular, steady, high-speed signals, as desired during the tuning process, as well as for verifying system operation.

Other types of transmit modes, which may be provided as part of the firmware or software of the sensor transmitter, and which may be utilized selectively during the operation of said sensor transmitter, may include 'burst" transmit modes, wherein a burst of data information is transmitted, or "parcel" transmit modes, wherein timed data packets of data, which may, as desired, comprise partial data strings, are transmitted, and, if desired, repeated during time intervals. Further, the sensors may have programmed therein diagnostic routines or other test modes which assist during manufacture and use, providing the operator with operational status and verification information on said sensor/transmitter, as needed.

Referring to **Figure 4**, the fire/security, or control panel **1**, by contrast with the sensor transmitter, which has little or no personality data, includes a data base 4l which contains the desired transmitter personality data, as well as, the address/device ID bits for each said transmitter. This data

can be programmed at the site, or at the factory, as desired.

Such personality data can be any combination of: transmitter TYPES, such as passive infrared, smoke detector, keypad, contact input, etc; transmitter PROPERTY/SYSTEM code which is common to all elements of a system to prevent adjacent but separate systems from interfering with one another; FREQUENCY CHANNEL or SPREAD SPECTRUM CDMA CODE, which is also typically common to all elements of a system for the same reason; there are also programmable functioning such as number of redundant alarm transmissions, alarm transmission separation, supervision interval timing, calibration factors and the like; there is also sensor input condition such as normally open/normally closed charge detect, debounce time, cut alarm wire detection or the like.

The greater this programmable personality information becomes, the more subtle the effects of unauthorized re-programming are and as a result, the more secure the programming method must be.

Each transmitter must be programmed with this information in order for it to function in the system. Returning to **Figure 4**, the fire/security, or control panel **4C**, or a separate programming device, is connected to the transmitter **4A** either directly through a wire cable **4H** or through an intermediate hand-held programmer **4D** via link **4F** which programmer is then connected to the transmitter **4A** through a wire cable **4G**. The hand-held programmer can be either electrically programmed by the fire/security, or control panel or operator. The programmer can receive data and provide visual indicia via the fire/security, or control panel **4K**, to key in programming commands **4D**, or the programming device can be self sufficient, configured to communicate with said fire/security, or control panel as well as said sensor or transmitter.

Alternately, an electromagnetic field **2**, in the form of, for example, a magnetic loop induction coil, or optical data link **3** can replace the wire cable, as shown in **Figure 3**. The electromagnetic or optical programming would be facilitated by a magnetic, electromagnetic **3A** or optical **3E** pick-up device. Those received signals are amplified by amplifier **3B**. Additionally, amplifier **3B** can be biased into a very low current or no current state to reduce power. This has the desirable effect of requiring a larger peak to peak voltage swing on pickup **3A**. This forces a programming device to be physically close access to a sensor element and reduces the chance of tampering or unauthorized operation. Further, the sensor or transmitter can be programmed to "wake up", "power up", handshake with the programming device and go into a programming mode upon exposure, via magnetic loop induction coil, of a electromagnetic field of a predetermined field strength, or exceeding said predetermined field strength.

This "wake up" feature allows the sensor transmitter to "sleep" during non-use or non-programming, and is initiated into the "wake up" mode by certain predesignated events, such as exposure to the inductive loop, above, or other external events, or internal events, such as, for example, timer, programmable counter, etc. Upon initiation into the "wake up" mode, a sequence of events occurs, including powering up, handshake protocol, if it believes a programming device is attempting to communicate, then programming protocol. Also, a self diagnostic and reporting transmission may

be provided, as desired. This sequence of events feature provides the ability to allow the sensor transmitter to respond to a programming device, while maintaining low power consumption.

Utilization of an inductive field coil for programming can have the additional advantage, with an appropriately configured sensor, of providing power to said transmitter via said magnetic or electromagnetic field **2**, during at least the programming phase, which may be a power-intensive application. While it has been known in other applications that a magnetic coil can be utilized to provide inductive power to devices, it is believed that such usage in the present application would be unique and, combined with the power up sequence above, is especially useful.

Likewise, as mentioned supra, the sensor can be configured so as to "power up", or "wake up" then "power up", handshake, and go into a programming mode upon exposure, via optical input **3**, of light of a predetermined brightness, frequency, modulation rate, or other variance. Additionally said photo detector **3E** can be include or be combined with photo generative power means, such as, for example, photo cells or the like to utilize said light generated by said optical input to provide power to said transmitter during at least the programming phase, which may be a power-intensive application.

The output of amplifier **3B** is then decoded by I/O decoder **3C** to determine 1/0 logic levels, as well as, both clock and data information **4**. Many such methods are commonly available including ratio encoding, Manchester encoding, Non-Return to Zero (NRZ) encoding, or the like; alternatively, a UART type approach can be used. Once so converted, clock and data signals containing the serial programming information bits are passed to memory means **3D**.

Any of these connection means resultingly provides a logical link from the fire/security, or control panel's internal data base **4I** to the sensor/transmitter **4A** to be programmed, as shown in **Figure 4**.

Continuing with **Figure 4,** prior to programming, the fire/security, or control panel **4C** chooses the necessary programmable transmitter functions and stores them into its data base **4I**. Next, a transfer of the fire/security, or control panel desired programming must be sent to the sensor or transmitter **4A**. In order to insure that an unauthorized user cannot connect into and program the transmitter **4A** the following procedure may be used:

Both the transmitter **4A** and receiver **4B** contain an identical, repeatable pseudo randomization algorithm in ROM or in ASIC logic. Referring to **Figure 5**, the algorithm is applied to outgoing programming data **5D** from the fire/security, or control panel **5A** and produces a number of security/randomization bits **5C** which are appended to the outgoing programming message or message **5D** and sent to the transmitter **5B**.

Referring to **Figure** 1 the transmitter likewise applies this pseudo randomization algorithm as the security/randomization bits (Fig 5. 5C) to the outgoing programming data (Fig 5, 5D), now forming the incoming programming data **1A** to the transmitter (Fig 5, 5B) and produces a several bit result in the shift register **1F**. The scrambling algorithm is devised such that a small difference in the programming bit stream causes a great difference in the pseudo randomization result. The present invention uses a

16 bit polynomial to produce this pseudo randomization.

Before the transmitter will accept this programming, stored in the address and personality register **1E**, both the pseudo random code, stored in the data in shift register **1G** from the fire/security, or control panel and the transmitter, in shift register **1F** must match via comparitor **1D**, indicating unauthorized acceptance use. In addition to insuring authorized access, this process also insures that the data itself is correct. The longer the polynomial sequence used, the greater the security.

A preferred embodiment of the present invention, utilizing spread spectrum or other RF transmission means should include a programming means to determine that the frequency or spread spectrum code is unique to the area. If a spread spectrum code, system code, or frequency channel is found to be occupied at a future time of use, then the system should be programmed to re-program the sensors and central processor unit so as to alter the programming such that a new, unused spread spectrum code or system code or frequency channel can be selected, or, in the alternative, the control panel of the central processor unit can alert the programmer to re-program the system to accomplish the same task.

To further increase security of the fire/security, or control system, not all systems have to operate on the same randomization code. The randomization seed **1H** can be altered occasionally. This would further prevent the theft of a programming device from providing an avenue to potentially compromise already installed fire/security, or control systems. Methods may be established from time to time to change the SEED **1H** of the pseudo randomization algorithms to further increase security. The present invention uses a complex polynomial to produce the desired randomization which includes a base randomization SEED **1H**. Alternatively, a less secure system could use a simple numeric sum of the bits or sum of the bytes.

Continuing with **Figure 4**, an alternative means of enhancing programming security, which may be utilized, would comprise the steps of:

a. placing a programming device **4D** in a programming mode, selectively generating a random seed, and communicating said seed into the memory of said central processing unit or fire/security, or control panel **4C** and said programming device **4D**, said random seed to be utilized in the validation of data transmitted all sensor/transmitters utilized in the alarm system to said fire/security, or control panel **4C** or central processing unit, providing a unique, site-specific operational code for said sensor array;

b. placing said programming device **4D** within the reception range of a sensor **4A**;

c. placing said sensor **4A** into a mode by which it can accept data via transmitted programming information from said programming device **4D**;

d. transmitting said seed from said programming device **4D** to said sensor/transmitter **4A** as part of a programming message, which programming message may also include the sensor address/ID code, type code, property code, transmitter timing, and spread spectrum channel, as shown, for example in **Figure 5**. Said sensor/transmitter could include EEROM as the

memory means, for example, which could be partitioned to allow for redundantly saving said seed and programming data in said EEROM, thereby providing a backup of said programming data upon corruption of part of the memory of said sensor transmitter.

Referring to **Figures 6a** and **6b**, the use of an EEROM (Electrically Erasable Read Only Memory) device in a circuit whose power supply varies unpredictably from, for example, 0 to 5 volts, with the voltage changing at varying rates from very slow (for example, days) to very fast (microseconds) represents many challenges. Although the EEROM devices are designed to maintain date without power present, and to allow reading and writing of data while power is present, do not always perform correctly when operated with variable power systems.

To prevent loss of data under such circumstances, three techniques may be implemented. The first may comprise removing power from the EEROM entirely unless it is desired to operate it. This prevents mis-operation at other times. The power switch may be programmed into the system, and may take the form, as shown in **Figure 6a**, of a pass transistor t in series with the EEROM's Ucc power lead, or, as shown in **Figure 6b**, the utilization of a logic gate L whose logic high output is capable of conveying sufficient power to the EEROM.

It is important to switch the power both on and off quickly, and both of the above power switching techniques above accomplish satisfactorily fast switching as desired.. However, the pass transistor of **Figure 6a** requires the addition of a load resistor r from Ucc to ground for satisfactory operation under these parameters.

Another technique is to avoid writing to the EEROM unless the software deems that is reasonable to expect that the power will be steady during operation, such as when the programming device is engaged.

A third technique is to store multiple, such as, for example, four copies of the data, each with an error detection code, to allow for determination of the integrity of the data upon later retrieval, thereby providing redundant memory storage of important data. Thus, if an individual "write operation"is disturbed, terminated, or otherwise corrupted by power variations or other means, the redundant storage provides back up data.

Returning now to **Figure 4**, step "e" would include, for example, the step of said sensor/transmitter **4A** inputting said programming message and saving said seed in memory;

f. said sensor/transmitter **4A** utilizing said seed to code digital data bits transmitted **4E** from said sensor/transmitter **4A** to said fire security panel **4C** or central processor unit, said central processor unit programmed to validate said data upon receipt of said code, and reject digital data received which does is not coded by said seed, thereby providing a unique, independent, site-specific operational code for each array site forming each alarm system; also included could be the further step of said sensor transmitting a verification burst upon completion of programming, said verification burst comprising a digital data string verifying the address/ID Code, type code, property code, transmitter timing, spread spectrum channel, and seed, after which there could be further included the step of said

programming device **4D** or said fire/security, control panel **4C** receiving said verification burst and verifying the digital data received, and upon verification, transmitting a JAM command addressed to the verified sensor, said JAM command placing said sensor in an un-programmable condition, such as, for example, putting the programming function into a loop, preventing unauthorized tampering of said verified transmitter. The JAM command is further discussed infra, and said methodology can be applied in the present teaching.

g. repeating steps b-f until all of said sensor transmitters in said array forming the alarm system have been programmed.

As earlier indicated, the sensor transmitters and said central processor unit could utilized for example, the CRC (cyclic redundancy check) coding method or check sum.

The data transmitted by said security/transmitter may be coded by appending said seed to said digital data bits, and wherein said central processor unit validates or rejects received upon detection of said seed string appended to said digital data bits, or, in the alternative, said digital data bits may be coded and decoded by applying a scrambling algorithm utilizing said seed.

As earlier indicated, the programming device may be configured to transmit data to said sensor utilizing a variety of alternative transmission means, including, for example, RF, IR, optical, or a magnetic loop/induction system, and wherein said sensor is configured to be shipped in a non-programmable mode, and is configured only to initiate programming sequence only upon exposure to a magnetic field of predetermined field strength, generated by said magnetic loop/induction system.

Further, the random seed may be communicated to said programming device via scanning a bar code, manual input, magnetic strip, or random number generation.

Returning to **Figure 4,** once the transmitter **4A** accepts the programming as correct, it then either transmits **4E** one or more verification messages or repeats its programming through the electric, magnetic or optical link **4G, 4H**. In this manner the fire/security, or control data base can match and verify 100% correctness of the desired program.

The programming method of the present invention may include the further step of monitoring for the other utlization of the spread spectrum code, system code, or frequency channel, and upon discerning other use, re-initiating programming of said spread spectrum code, system code, or frequency of said sensor/transmitters and said central processing unit to change said spread spectrum code, system code, or frequency to an new spread spectrum code, system code, or frequency.

Once the programming connection is established with the transmitter, this link can also be used to aid in production of the transmitter. For example, special program commands can be used to test battery low or help automated tuning of transmitter elements. Further, this feature can be used in the field to insure full functionality of the device prior to installation.

An alternative embodiment of the present invention, wherein the transmitter would provide the security/randomization code, could work as follows:

a. placing an unprogrammed transmitter in near proximity to an unprogrammed

fire/security, or control receiver;

b. said receiver set into a mode by which it can accept programming data via transmitted programming information from said transmitter;

c. limiting the signal strength of said transmitter to a near proximity of the receiver or by way of a special bit in the transmitted message signifying that the message is a programming message;

d. said transmitter having a random number means for generating random numbers;

e. selectively generating a security/randomization bit for said transmitter by initiating said random number generator, and designating said random number generated as said security/randomization bit, and transmitting said bit to said receiver;

f. said receiver imputing programming message and determining if such a device ID/address already exists in the system;

g. If said new device ID/address is acceptable it becomes internally associated by the receiver or security/fire panel with the appropriate transmitter;

h. If the new device ID/address is not acceptable the receiver or fire/security, or control panel so makes an appropriate indication;

i. Step e is repeated until step h is met, once met the transmitter is removed from the programming mode.

The above method could include the additional step after step "e" of the receiver inputting said transmission and appending said security/randomization bit to programming data including new device ID/address, forming a programming message, and transmitting said programming message to said transmitter.

A programming button for initializing said random number generator as set forth in step "e"; in such an embodiment said programming button for generating said random number generator feature may be configured to reprogram after its use as a random number generator, to allow said switch to be utilized to program the spread spectrum code or frequency channel or the like, by depressing said button in increments for selecting the desired channel. For example, five depressions of the button could change the selected channel from one to five.

In such an embodiment, the ability to disable said programming button in order to prevent further tampering of the receiver once programmed would be desirable; such a means to disable could include, for example, switching the input protocol into a loop, preventing further input from said button.

Said programming button might also be utilized to set the transmitter type code in the transmitter for transmission to the receiver.

It is possible, in some applications, that the wire programming link or the magnetic field or optical programming link WILL NOT or COULD NOT be disconnected. Further, it is important that an unauthorized person COULD NOT AT A FUTURE POINT, after the initial programming of the transmitter,

alter that programming by simple re-connection of a programming cable. If the transmitter became re-programmed it would be possible for the transmitter to create false or unrecognizable information which would render the fire/security, or control system ineffective. This is especially true of more sophisticated systems which require extensive programmability of sensor/transmitter personality.

To facilitate these essential needs, the present invention provides a "JAM" **2C** function, as illustrated in **Figure 2**. Once the fire/security, or control panel verifies that the transmitter programming is indeed correct, a "JAM" command (Figure 5, 5E) can be sent. The incoming programming message is stored in memory means **2B** as shown in **Figure 2.** Referring again to **Figure 5**. the programming message is compared to a unique bit pattern **5C** which represents the JAM command. Referring again to **Figure 2**, once a match is verified **2D**, the JAM command is permanently latched into flip-flop **2E**. Alternatively, a fused link, EAROM, PROM or the like could be utilized. The JAM command logically disconnects the programming connection via logic circuit **2F** so that future incoming programming commands via programming input **2A** will be ignored. Alternatively, the JAM command could be replaced or augmented by a switch **2G** or a jumper located within the transmitter which disconnects the incoming programming commands via programming input **2A**.

Once the JAM sequence is initiated, any future attempt to compromise the system will be thwarted. This feature is ESSENTIAL for programming links which CANNOT BE DISABLED such as magnetic, electromagnetic or optical links. Magnetic, electromagnetic, or optical waves can effectively travel at great distances and would allow an unauthorized programmer off-sight ability to compromise the fire/security, or control system without detection.

As a further safeguard, it would be possible to additionally encrypt the programming message itself. This would provide increased security when programming using the magnetic, electromagnetic or optical links.

The optical or magnetic means of imputing programming do not have to directly interface with a portable programmer or with a fire/security, or control panel. Instead those inputs could directly sense the information contained on an optical or magnetic bar code or the like or the H field information on a magnetic strip.

In this manner, the bar code or magnetic strip could be coded or printed either at the time of manufacture, or at the time of installation and be optionally affixed to the sensor transmitter itself. Alternately, a sheet of pre-programmed bar codes with their associated meaning could be produced and distributed to fire/security system installers. In this manner the installer need only choose the appropriate personality features and addresses and pass them by the magnetic or optical input of the sensor. As a further option an electricity detachable bar code wand could be used to input the bar codes or magnetic strip.

Such a programming method has the advantage of needing no portable programmer, it is a non-volatile storage means and needs no electrical connection. The bar code or magnetic strip need only be passed by the magnetic or optical programming input of the sensors. A second bar code with

the JAM command could then terminate potential future programming.

All of the disclosed methods can be implemented as direct hardware blocks or with microprocessor software or with micro-coded state generators or the like.

The invention embodiments herein described are done so in detail for exemplary purposes only, and may be subject to many different variations in design, structure, application and operation methodology. Thus, the detailed disclosures therein should be interpreted in an illustrative, exemplary manner, and not in a limited sense.

CLAIMS

What is claimed is:

1. The method of programming an array of sensor transmitters to communicate with a central processing unit in a secure fashion, comprising the steps of:

a. placing a programming device in a programming mode, selectively generating a seed, and communicating said seed into the memory of said central processing unit and said programming device, said seed to be utilized in the validation of data transmitted from said sensor transmitters to said central processing unit, providing a unique operational code for said sensor transmitter array;

b. placing said programming device within the reception range of a sensor transmitter;

c. placing said sensor transmitter into a mode by which it can accept data via transmitted programming information from said programming device;

d. transmitting said seed from said programming device to said transmitter as part of a programming message;

e. said sensor transmitter inputting said programming message and saving said seed in memory;

f. said sensor transmitter utilizing said seed to code digital data bits transmitted from said sensor transmitter to said central processor unit, said central processor unit programmed to validate said data upon receipt of said code, and reject digital data received which does is not coded by said seed, thereby providing a unique operational code for said array site;

g. repeating steps b-f until all of said sensor transmitters in said array have been programmed.

2. The method of **Claim 1**, wherein said sensor transmitters and said central processor unit utilize the CRC (cyclic redundancy check) coding method.

3. The method of **Claim 1 or 2**, wherein in step "a" there is provided the additional step of said programming device appending to said data string containing said seed, and sending to said sensor transmitter and central processor unit, the sensor transmitter address/ID code, type code, system code, property code, and spread spectrum channel.

4. The method of **Claim 1, 2 or 3**, wherein after step "f" of **Claim 1**, there is included the further step of said sensor transmitter transmitting a verification burst upon completion of programming, said verification burst comprising a digital data string verifying said sensor transmitter's address/ID Code, type code, property code, spread spectrum channel, and seed.

5. The method of **Claim 4**, wherein there is included the additional step of verifying said

sensor transmitter's programming, and upon verification, transmitting a JAM command addressed to the verified sensor transmitter, said JAM command altering the programmability of said sensor transmitter, preventing unauthorized programming or tampering of said verified transmitter.

6. The method of **Claim 1, 2, 3, 4, or 5,** wherein said sensor transmitter has provided therein EEROM, and step "e" includes the further step of redundantly saving said seed and programming data in said EEROM, thereby providing a backup of said programming data upon corruption of part of the memory of said sensor transmitter, said EEROM further comprising error detection means for detecting errors in data stored in memory.

7. The method of **Claim 1, 2, 3, 4, 5, or 6,** wherein said sensor transmitter has provided therein EEROM, and there is further provided the additional step of utilizing a power means for limiting the operation of said EEROM.

8. The method of **Claim 7**, wherein said power means comprises a logic gate whose logic high output is capable of conveying sufficient power to the EEROM.

9. The method of **Claim 7**, wherein said power means comprises a pass transistor in series with the EEROM's Ucc power lead.

10. The method of **Claim 7, 8,** or **9**, wherein there is provided the additional step of providing EEROM limited programming means for limiting programming said EEROM to that period when said programming device is providing power to said sensor transmitter.

11. The method of **Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, or 10**, wherein in step "f" of **Claim 1**, said digital data bits are coded by appending said seed to said digital data bits, and wherein said central processor unit validates or rejects received upon detection of said seed string appended to said digital data bits.

12. The method of **Claim 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, or 11**, wherein, in step "f" of **Claim 1**, said digital data bits are coded and decoded by applying a scrambling algorithm utilizing said seed.

13. The method of **Claim 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, or 12**, wherein said programming device transmits data to said sensor transmitter utilizing a magnetic loop/induction system, and is configured only to initiate programming sequence only upon exposure to a magnetic field exceeding a predetermined field strength, generated by said magnetic loop/induction system.

14. The method of **Claim 13**, wherein said sensor transmitter is configured to utilize said magnetic field generated by said magnetic loop/induction system to power said sensor transmitter.

15. The method of **Claim 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, or 14**, wherein said programming device transmits data to said sensor transmitter utilizing an optical linkage, and is configured only to initiate programming sequence only upon exposure to light exceeding a predetermined parameter generated by said optical linkage.

16. The method of **Claim 15**, wherein said predetermined parameter is established by the brightness of said light.

17. The method of **Claim 15**, wherein said predetermined parameter is established by the frequency of said light.

18. The method of **Claim 15**, wherein said predetermined parameter is established by modulating said light at a predetermined modulation rate.

19. The method of **Claims 3, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, or 18**, wherein there is further included the step of monitoring for the unauthorized utlization of said spread spectrum code, and upon discerning unauthorized use, re-initiating programming of said spread spectrum code of said sensor/transmitters and said central processing unit to change said spread spectrum code to an new spread spectrum code.

20. The method of **Claims 3, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17,18, or 19**, wherein there is further included the step of monitoring for the unauthorized utlization of said system code, and upon discerning unauthorized use, re-initiating programming of said system code of said sensor/transmitter and said central processing unit to change said system code to a new system code.

21. The method of **Claims 1, 2, 3, 4, 7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 29, or 20**, wherein the data is transmitted via radio frequency having a frequency channel, and wherein there is further included the step of monitoring for the unauthorized utlization of said frequency channel, and upon discerning unauthorized use, re-initiating programming of said sensor/transmitters and said central processing unit to a new frequency channel.

22. The method of **Claim 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, or 21** wherein in step "a" of Claim 1, said seed is communicated to said programming device via scanning a bar code.

23. The method of **Claim 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, or 21**, wherein in step "a" of Claim 1, said seed is communicated to said programming device via reading a magnetic strip.

24. The method of **Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, or 23**, wherein said sensor transmitter has programmed power conservation means, said power conservation means for switching said sensor transmitter into a power saving mode, and wherein there is included the additional steps in step "c" of said sensor transmitter waking up upon contacting said programming device, then said sensor transmitter, powering up, handshaking with said programming device, and then being placed into a programming mode to accept programming from said programming device.

25. The method of **Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, or 24**, wherein said sensor transmitter further comprises transmit condition variance means for varying the speed and/or time period of transmission, selective increasing or decreasing the speed of transmission, or selectively transmitting in a continuous mode, burst mode, parcel mode, or other desired transmission rate.

26. The method of **Claim 25**, wherein there is provided the further step of providing self diagnostic means for said sensor transmitter for diagnosing the condition and operability of said sensor transmitter, and there is provided the step of selectively initiating said self diagnostic means, and verifying that said sensor transmitter is functioning within acceptable parameters.

27. The method of programming a sensor transmitter in a secure manner, comprising the steps of:

a. providing a programming device containing sensor transmitter identification and function information comprising programming data bits, said programming device further containing in memory a scrambling algorithm;

b. providing a sensor transmitter containing a scrambling algorithm compatible with said programming device scrambling algorithm;

c. said programming device applying said scrambling algorithm to said programming data bits, producing security/randomization bits which are appended to said programming data bits, forming an outgoing programming message having programming data bits and appended security/randomization bits;

d. transferring said outgoing programming message from said programming device to said sensor transmitter, forming an incoming programming message to said sensor transmitter;

e. said sensor transmitter applying said scrambling algorithm to said incoming data bits in said

incoming programming message, providing a scrambling result;

f. comparing said scrambling result to the security/randomization bits appended to said programming data bits in said incoming programming message;

g. upon a correct match of said scrambling result with said security/randomization bits, said sensor transmitter/transmitter accepting said programming data bits in said incoming programming message from said programming device as from a valid, secure programming device, and

h. said sensor transmitter transmitting a verification message verifying valid programming.

28. The method of **Claim 27** whereby the linking of said programming station to said sensor transmitter is accomplished magnetically or optically.

29. The method of **Claim 27**, wherein, following step "g", there is included the additional step of said programming station, once verifying that said sensor transmitter has been successfully programmed, said programming station sending a coded JAM command to said sensor transmitter, said sensor transmitter permanently latching said jam command into a flip-flop in such a manner as to logically disconnect the programming connection for said sensor transmitter so that future incoming programming commands received by said sensor transmitter will be ignored.

30. The method of **Claim 27,** wherein there is provided the additional step in step "c" of said programming station, encrypting said programming data bits, and said sensor transmitter decrypting said programming data bits.

31. The method of **Claim 27**, wherein said security/randomization bits are communicated to said programming device via optical data link, said optical data link further including the steps of reading a bar code.

32. The method of **Claim 27**, wherein said security/randomization bits are communicated to said programming device via reading a magnetic stripe.

33. The method of **Claims 27, 28, 29, 30, 31, or 32**, wherein there is further included the step of monitoring for the unauthorized utlization of said spread spectrum code, and upon discerning unauthorized use, re-initiating programming of said spread spectrum code of said sensor/transmitters and said central processing unit to change said spread spectrum code to an new spread spectrum code.

34. The method of **Claims 27, 28, 29, 30, 31, 32, or 33**, wherein there is further included the step of monitoring for the unauthorized utlization of said system code, and upon discerning unauthorized

use, re-initiating programming of said system code of said sensor/transmitters and said central processing unit to change said system code to an new system code.

35. The method of **Claims 27, 28, 29, 30, 31, 32, 33, or 34**, wherein the programming message of step "d" is transferred via radio frequency having a frequency channel, and wherein there is further included the step of monitoring for the unauthorized utlization of said frequency channel, and upon discerning unauthorized use, re-initiating programming of said sensor/transmitters and said central processing unit to a new frequency channel.

36. The method of **Claim 27, 28, 29, 30, 31, 32, 33, 34, or 35**, wherein after step "f" of **Claim 27**, there is included the further step of said sensor transmitter transmitting a verification burst upon completion of programming, said verification burst comprising a digital data string verifying said sensor transmitter's address/ID Code, type code, property code, spread spectrum channel, and seed.

37. The method of **Claim 36**, wherein said verification burst includes a data string indicating status conditions of said sensor transmitter.

38. The method of programming a sensor transmitter in a secure manner, comprising the steps of:

a. providing sensor transmitter identification and function information comprising programming data bits;

b. applying a scrambling algorithm to said programming data bits, producing security/randomization bits, appending said security/randomization bits to said programming data bits, forming a programming message having programming data bits and security/randomization bits;

c. providing a sensor transmitter containing in memory a scrambling algorithm compatible to said scrambling algorithm in step "b";

d. transferring said programming message to said sensor transmitter, forming an incoming programming message to said sensor transmitter;

e. said sensor transmitter applying said scrambling algorithm in said memory to said incoming programming data bits in said incoming programming message, providing a scrambling result;

f. comparing said scrambling result to the security/randomization bits appended to said programming data;

g. upon a correct match of said scrambling result with said security/randomization bits, said sensor transmitter accepting said data bits in said incoming programming message as from a valid, secure programmer, and

h. upon verification of a secure programmer, said sensor transmitter accepting said data from said programming device.

39. The method of **Claim 38**, wherein there is included the further step of said sensor transmitter transmitting a verification burst upon completion of programming, said verification burst comprising a digital data string verifying said sensor transmitter's address/ID Code, type code, property code, spread spectrum channel, and seed.

40. The method of **Claims 38 or 39**, wherein there is included the additional step of verifying said sensor transmitter's programming, and upon verification, transmitting a JAM command addressed to the verified sensor transmitter, said JAM command preventing unauthorized tampering of said verified transmitter.

41. The method of **Claim 38** whereby the linking of said programming station to said sensor transmitter is accomplished magnetically or optically.

42. The method of **Claim 38**, whereby there is further included, after step "g", the additional step of sending a coded JAM command to said sensor transmitter, said sensor transmitter comparing said JAM command with said programming message and, upon verifying a match, said sensor transmitter permanently latching said jam command into a flip-flop in such a manner as to logically disconnect the programming connection so that future incoming programming command will be ignored.

43. The method of **Claim 38**, wherein there is provided the additional step in step "b" of encrypting said programming data bits, and wherein there is provided the additional step in step "e" of said sensor transmitter decrypting said encrypted programming data bits.

44. The method of **Claim 38**, wherein said verification burst includes a sensor transmitter identification code and power status.

45. The method of **Claim 38**, said programming message in step "b" is stored and scanned from a bar code.

46. The method of **Claim 38**, wherein said programming message in step "b" is stored and read from a magnetic strip.

47. The method of **Claim 38**, wherein said programming station is portable.

48. The method of **Claim 38**, wherein said programming station is part of a receiver or control panel.

49. The method of **Claims 39 or 40**, wherein there is further included the step of monitoring for the unauthorized utlization of said spread spectrum code, and upon discerning unauthorized use, re-initiating programming of said spread spectrum code of said sensor/transmitters and said central processing unit to change said spread spectrum code to an new spread spectrum code.

50. The method of **Claims 39 or 40**, wherein there is further included the step of monitoring for the unauthorized utlization of said system code, and upon discerning unauthorized use, re-initiating programming of said system code of said sensor/transmitters and said central processing unit to change said system code to an new system code.

51. The method of **Claims 38, 39, or 40**, wherein the data is transmitted via radio frequency having a frequency channel, and wherein there is further included the step of monitoring for the unauthorized utlization of said frequency channel, and upon discerning unauthorized use, re-initiating programming of said sensor/transmitters and said central processing unit to a new frequency channel.

52. The method of programming a sensor transmitter in a secure manner, comprising the steps of:

a. providing sensor transmitter identification and function information comprising programming data bits;

b. applying a scrambling algorithm to said programming data bits, producing security/randomization bits, appending said security/randomization bits to said programming data bits, forming a programming message having programming data bits and security/randomization bits;

c. providing a sensor transmitter containing in memory a scrambling algorithm compatible to said scrambling algorithm in step "b";

d. transferring said programming message to said sensor transmitter, forming an incoming programming message to said sensor transmitter;

e. said sensor transmitter applying said scrambling algorithm in said memory to said incoming programming data bits in said incoming programming message, providing a scrambling result;

f. comparing said scrambling result to the security/randomization bits appended to said programming data;

g. upon a correct match of said scrambling result with said security/randomization bits, said transmitter accepting said data bits in said incoming programming message as from a valid, secure programmer.

h. sending a coded JAM command to said sensor transmitter, said sensor transmitter comparing said JAM command with said programming message and, upon verifying a match, said sensor transmitter initiating a means to disconnect the programming connection, preventing further

programming of said sensor transmitter.

53. The method of **Claim 52** whereby the linking of said programming station to said sensor transmitter is accomplished magnetically or optically.

54. The method of **claim 52**, whereby said scrambling algorithm may be alterable.

55. The method of **Claim 52**, wherein there is provided the additional step in step "b" of encrypting said programming data bits, and in step "e" said sensor transmitter decrypting said encrypted programming data bits.

56. The method of **Claim 52**, wherein there is included after step "g" the additional step of said transmitter sending a verification burst to the programmer.

57. The method of **Claim 52**, said programming message in step "b" is stored on a bar code.

58. The method of **Claim 52**, wherein said identification and function information in step "a" is stored on a magnetic strip.

59. The method of **Claim 52**, wherein said programming station is portable.

60. The method of **Claim 52**, wherein said programming station is part of a control panel.

61. The method of **Claim 52**, wherein there is included the further step of said sensor transmitter transmitting a verification burst upon completion of programming, said verification burst comprising a digital data string verifying said sensor transmitter's address/ID Code, type code, property code, spread spectrum channel, and seed.

62. The method of **Claim 61**, wherein there is further included the step of monitoring for the unauthorized utlization of said spread spectrum code, and upon discerning unauthorized use, re-initiating programming of said spread spectrum code of said sensor/transmitters and said central processing unit to change said spread spectrum code to an new spread spectrum code.

63. The method of **Claim 61**, wherein there is further included the step of monitoring for the unauthorized utlization of said system code, and upon discerning unauthorized use, re-initiating programming of said system code of said sensor/transmitters and said central processing unit to change said system code to an new system code.

64. The method of **Claims 52, 53, 54, 55, 56, 57, 58, 59, 60, or 61**, wherein the data is transmitted via radio frequency having a frequency channel, and wherein there is further included the step of monitoring for the unauthorized utlization of said frequency channel, and upon discerning unauthorized use, re-initiating programming of said sensor/transmitters and said central processing unit to a new frequency channel.

65. A method of programming a sensor transmitter in a secure fashion, comprising the steps of:

a. placing an unprogrammed sensor transmitter in near proximity to an unprogrammed system receiver/panel/programming device;

b. said receiver set into a mode by which it can accept programming data via transmitted programming message from said sensor transmitter;

c. limiting the signal strength of said sensor transmitter to a near proximity of the receiver;

d. selectively generating security/randomization bits for said sensor transmitter, and transmitting said bits to said receiver;

e. said receiver imputing programming message and determining if such a device ID/address already exists in the system;

f. if said new device ID/address is acceptable it becomes internally associated by the system receiver/panel/programming device with said sensor transmitter;

g. if the new device ID/address is not acceptable the receiver or system receiver/panel/programming device so makes an appropriate indication;

h. steps d-g are repeated until step h is met, once met the transmitter is removed from the programming mode.

66. The method of programming a sensor transmitter/transmitter of **Step 65**, wherein after step "g" there is provided the additional step of said receiver inputting said transmission and appending said security/randomization bit to programming data including new device ID/address, forming a programming message, and sending said programming message to said transmitter;

67. The method of programming a sensor transmitter/transmitter of **Step 65** wherein in step "d" there is included the extra step of providing input means for externally inputting said security/randomization bit.

68. The method of programming a sensor transmitter/transmitter of **Claim 65** wherein, once the device ID/address is programmed with the transmitter, said programming button for generating said random number generator feature is configured to reprogram to allow said switch to be utilized to program the spread spectrum code or frequency channel or the like, by depressing said button in

increments for selecting the desired channel.

69. The method of programming a sensor transmitter/transmitter of **Claim 65,** wherein there is provided the additional step of the transmitter type code is transferred from the transmitter to said receiver for programming of said receiver.

70. The method of **Claim 65**, wherein there is included the further step of said sensor transmitter transmitting a verification burst upon completion of programming, said verification burst comprising a digital data string verifying said sensor transmitter's address/ID Code, type code, property code, spread spectrum channel, and seed.

71. The method of **Claim 70**, wherein there is further included the step of monitoring for the unauthorized utlization of said spread spectrum code, and upon discerning unauthorized use, re-initiating programming of said spread spectrum code of said sensor/transmitters and said central processing unit to change said spread spectrum code to an new spread spectrum code.

72. The method of **Claim 70**, wherein there is further included the step of monitoring for the unauthorized utlization of said system code, and upon discerning unauthorized use, re-initiating programming of said system code of said sensor/transmitters and said central processing unit to change said system code to an new system code.

73. The method of **Claims 65, 66, 67, 68, 69, or 70**, wherein the data is transmitted via radio frequency having a frequency channel, and wherein there is further included the step of monitoring for the unauthorized utlization of said frequency channel, and upon discerning unauthorized use, re-initiating programming of said sensor/transmitters and said central processing unit to a new frequency channel.

74. The method of programming an array of sensor transmitters to communicate with a central processing unit in a secure fashion, comprising the steps of:

a. providing a EEROM power means for selectively switching power to a sensor transmitter EEROM, limiting the operation of said EEROM to predetermined periods;

b. placing a programming device in a programming mode;

c. placing said sensor transmitter into a mode by which it can accept data via transmitted programming information from said programming device;

d. utilizing said EEROM power means to switch on programming power to said sensor transmitter EEROM, placing said EEROM in a programming mode

e. transmitting programming data from said programming device to said transmitter as part

of a programming message;

f. said sensor transmitter inputting said programming message and saving said programming data in memory;

g. once programming ceases, utilizing said EEROM power means for switching off designated programming power to said EEROM, thereby conserving power.

h. repeating steps b-h until all of said sensor transmitters in said array have been programmed.

75. The method of **Claim 74** wherein there is included the further step of redundantly saving said seed and programming data in said EEROM, thereby providing a backup of said programming data upon corruption of part of the memory of said sensor transmitter, said EEROM further comprising error detection means for detecting errors in data stored in memory.

76. The method of **Claim 75**, wherein said EEROM power means comprises a logic gate whose logic high output is capable of conveying sufficient power to the EEROM.

77. The method of **Claim 75**, wherein said EEROM power means comprises a pass transistor in series with the EEROM's Ucc power lead.

78. The method of **Claim 75, 76, or 77**, wherein there is provided the additional step of providing EEROM limited programming means for limiting programming of said EEROM to that period when said programming device is providing power to said sensor transmitter.

79. The method of **Claim 74, 75, 76, 77, or 78,** wherein said sensor transmitter has programmed therein power conservation means, said power conservation means for switching said sensor transmitter into a power saving mode, and wherein there is included the additional steps in step "c" of said sensor transmitter waking up upon contacting said programming device, then said sensor transmitter, powering up, handshaking with said programming device, and then being placed into a programming mode to accept programming from said programming device.

80. The method of **Claim 74, 75, 76, 77, 78, or 79**, wherein said programming device transmits data to said sensor transmitter utilizing a magnetic loop/induction system, and is configured only to initiate programming sequence only upon exposure to a magnetic field exceeding a predetermined field strength, generated by said magnetic loop/induction system.

81. The method of **Claim 80**, wherein said sensor transmitter is configured to utilize said magnetic field generated by said magnetic loop/induction system to power said sensor transmitter.

82. The method of **Claim 74, 75, or 76**, wherein after step "f" of **Claim 74**, there is included the further step of said sensor transmitter transmitting a verification burst upon completion of programming, said verification burst verifying correct programming of said sensor transmitter.

83. The method of **Claim 82** wherein there is included the additional step of verifying said sensor transmitter's programming via said verification burst, and upon verification, transmitting a JAM command addressed to the verified sensor transmitter, said JAM command altering the programmability of said sensor transmitter, preventing unauthorized programming or tampering of said verified transmitter.

84. The method of programming an array of sensor transmitters to communicate with a central processing unit in a secure fashion, comprising the steps of:

a. providing a programming device having an magnetic loop coil;

b. placing a programming device in a programming mode;

c. providing a sensor transmitter with power conservation means, said power conservation means including a low power mode and a high power mode, and switching means for switching from a lower power mode to a high power mode, and visa-versa, said sensor transmitter further having magnetic field sensing means for sensing a predesignated magnetic field;

d. setting said magnetic loop coil to emit a predesignated magnetic field strength, and placing said magnetic loop coil into the reception range of said magnetic field sensing means;

e. upon sensing a predesignated magnetic field, said magnetic field sensing means switching said power conservation means from a low power mode to a high power mode, placing said sensor transmitter into a mode by which it can accept data via transmitted programming information from said programming device;

f. transmitting programming data from said programming device to said transmitter as part of a programming message;

g. said sensor transmitter inputting said programming message and saving said programming data in memory;

h. once programming ceases, utilizing said power conservation means for switching said sensor to a lower power mode, thereby conserving power.

i. repeating steps b-h until all of said sensor transmitters in said array have been programmed.

85. The method of **Claim 84**, wherein there is provided the additional step of said sensor transmitter utilize said magnetic field generated by said magnetic loop/induction system to power said sensor transmitter.

86. The method of **Claim 84**, wherein after step "g" of **Claim 1**, there is included the further step of said sensor transmitter transmitting a verification burst upon completion of programming, said verification burst verifying correct programming of said sensor transmitter.

87. The method of **Claim 86**, wherein there is included the additional step of verifying said sensor transmitter's programming via said verification burst, and upon verification, transmitting a JAM command addressed to the verified sensor transmitter, said JAM command altering the programmability of said sensor transmitter, preventing unauthorized programming or tampering of said verified transmitter.

88. The method of **Claims 84, 85, 86, 87, or 88**, wherein said sensor transmitter further comprises transmit condition variance means for varying the speed and/or time period of transmission, and wherein there is further included the step of selectively varying the speed of transmission or selectiively transmitting in a continuous mode, burst mode, parcel mode, or other desired transmission rate.

89. The method of **Claims 84, 85, 86, 87, 88, or 89**, wherein said sensor transmitter further comprises transmit condition variance means for varying the speed and/or time period of transmission, and wherein there is further included the step of selectiively transmitting in a continuous mode, burst mode, or parcel mode.

90. The method of **Claim 84**, wherein there is provided the further step of providing self diagnostic means for said sensor transmitter for diagnosing the condition and operability of said sensor transmitter, and there is provided the step of selectively initiating said self diagnostic means, and verifying that said sensor transmitter is functioning within acceptable parameters.

91. The method of programming an array of sensor transmitters to communicate with a central processing unit in a secure fashion, comprising the steps of:

a. providing a programming device having an optical data link;

b. placing a programming device in a programming mode;

c. providing a sensor transmitter with power conservation means, said power conservation means including a low power mode and a high power mode, and switching means for switching from a lower power mode to a high power mode, and visa-versa, said sensor transmitter further having an optical input and optical sensing means for sensing a optical emission;

d. setting said optical data link of said programming device to emit a predesignated optical emission, and placing said optical input of said sensor into the reception range of said optical data link;

e. upon sensing a predesignated optical emission, said optical sensing means switching said power conservation means from a low power mode to a high power mode, placing said sensor transmitter into a mode by which it can accept data via transmitted programming information from said programming device;

f. transmitting programming data from said programming device to said transmitter as part of a programming message;

g. said sensor transmitter inputting said programming message and saving said programming data in memory;

h. once programming ceases, utilizing said power conservation means for switching said sensor to a lower power mode, thereby conserving power.

i. repeating steps b-h until all of said sensor transmitters in said array have been programmed.

92. The method of **Claim 91**, wherein there is provided the additional step of said sensor transmitter utilizing said optical emission generated by said optical data link power said sensor transmitter.

93. The method of **Claim 91**, wherein after step "g" of **Claim 91**, there is included the further step of said sensor transmitter transmitting a verification burst upon completion of programming, said verification burst verifying correct programming of said sensor transmitter.

94. The method of **Claim 93**, wherein there is included the additional step of verifying said sensor transmitter's programming via said verification burst, and upon verification, transmitting a JAM command addressed to the verified sensor transmitter, said JAM command altering the programmability of said sensor transmitter, preventing unauthorized programming or tampering of said verified transmitter.

95. The method of **Claims 91, 92, 93, or 94**, wherein said sensor transmitter further comprises transmit condition variance means for varying the speed of transmission, and there is included the additional step of selectively varying the speed of transmission.

96. The method of **Claims 91, 92, 93, or 94**, wherein said sensor transmitter further comprises transmit condition variance means for varying the time period of transmission, and wherein there is included the step of selectively transmitting in a continuous mode, burst mode, parcel mode, or other desired transmission rate.

97. The method of **Claims 95 or 96**, wherein there is provided the further step of providing self

diagnostic means for said sensor transmitter for diagnosing the condition and operability of said sensor transmitter, and there is provided the step of selectively initiating said self diagnostic means, and verifying that said sensor transmitter is functioning within acceptable parameters.

AMENDED CLAIMS

[received by the International Bureau on 17 October 1995 (17.10.95);
original claims 3, 4, 6, 7, 10, 11, 13, 15, 19-25,
34-36, 40, 79, 80, 88, 89 and 97 amended;
remaining claims unchanged (16 pages)]

1. The method of programming an array of sensor transmitters to communicate with a central processing unit in a secure fashion, comprising the steps of:

a. placing a programming device in a programming mode, selectively generating a seed, and communicating said seed into the memory of said central processing unit and said programming device, said seed to be utilized in the validation of data transmitted from said sensor transmitters to said central processing unit, providing a unique operational code for said sensor transmitter array;

b. placing said programming device within the reception range of a sensor transmitter;

c. placing said sensor transmitter into a mode by which it can accept data via transmitted programming information from said programming device;

d. transmitting said seed from said programming device to said transmitter as part of a programming message;

e. said sensor transmitter inputting said programming message and saving said seed in memory;

f. said sensor transmitter utilizing said seed to code digital data bits transmitted from said sensor transmitter to said central processor unit, said central processor unit programmed to validate said data upon receipt of said code, and reject digital data received which does is not coded by said seed, thereby providing an operational code for said array site;

g. repeating steps b-f until all of said sensor transmitters in said array have been programmed.

2. The method of **Claim 1**, wherein said sensor transmitters and said central processor unit utilize the CRC (cyclic redundancy check) coding method.

3. The method of **Claim 1**, wherein in step "a" there is provided the additional step of said programming device appending to said data string containing said seed, and sending to said sensor transmitter and central processor unit, the sensor transmitter address/ID code, type code, system code, property code, and spread spectrum channel.

4. The method of **Claim 1**, wherein after step "f" of **Claim 1**, there is included the further step of said sensor transmitter transmitting a verification burst upon completion of programming, said verification burst comprising a digital data string verifying said sensor transmitter's address/ID Code, type code, property code, spread spectrum channel, and seed.

5. The method of **Claim 4**, wherein there is included the additional step of verifying said

sensor transmitter's programming, and upon verification, transmitting a JAM command addressed to the verified sensor transmitter, said JAM command altering the programmability of said sensor transmitter, preventing unauthorized programming or tampering of said verified transmitter.

6. The method of **Claim 1,** wherein said sensor transmitter has provided therein EEROM, and step "e" includes the further step of redundantly saving said seed and programming data in said EEROM, thereby providing a backup of said programming data upon corruption of part of the memory of said sensor transmitter, said EEROM further comprising error detection means for detecting errors in data stored in memory.

7. The method of **Claim 6,** wherein said sensor transmitter has provided therein EEROM, and there is further provided the additional step of utilizing a power means for limiting the operation of said EEROM.

8. The method of **Claim 7**, wherein said power means comprises a logic cage whose logic high output is capable of conveying sufficient power to the EEROM.

9. The method of **Claim 7**, wherein said power means comprises a pass transistor in series with the EEROM's Ucc power lead.

10. The method of **Claim 9**, wherein there is provided the additional step of providing EEROM limited programming means for limiting programming said EEROM to that period when said programming device is providing power to said sensor transmitter.

11. The method of **Claim 1**, wherein in step "f" of **Claim 1**, said digital data bits are coded by appending said seed to said digital data bits, and wherein said central processor unit validates or rejects received upon detection of said seed string appended to said digital data bits.

12. The method of **Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, or 11**, wherein, in step "f" of **Claim 1**, said digital data bits are coded and decoded by applying a scrambling algorithm utilizing said seed.

13. The method of **Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, or 11**, wherein said programming device transmits data to said sensor transmitter utilizing a magnetic loop/induction system, and is configured only to initiate programming sequence only upon exposure to a magnetic field exceeding a predetermined field strength, generated by said magnetic loop/induction system.

14. The method of **Claim 13**, wherein said sensor transmitter is configured to utilize said magnetic field generated by said magnetic loop/induction system to power said sensor transmitter.

15. The method of **Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, or 11**, wherein said programming device transmits data to said sensor transmitter utilizing an optical linkage, and is configured only to initiate programming sequence only upon exposure to light exceeding a predetermined parameter generated by said optical linkage.

16. The method of **Claim 15**, wherein said predetermined parameter is established by the brightness of said light.

17. The method of **Claim 15**, wherein said predetermined parameter is established by the frequency of said light.

18. The method of **Claim 15**, wherein said predetermined parameter is established by modulating said light at a predetermined modulation rate.

19. The method of **Claims 3, 6, 7, 8, 9, 10, or 11**, wherein there is further included the step of monitoring for the unauthorized utlization of said spread spectrum code, and upon discerning unauthorized use, re-initiating programming of said spread spectrum code of said sensor/transmitters and said central processing unit to change said spread spectrum code to an new spread spectrum code.

20. The method of **Claims 3, 6, 7, 8, 9, 10, or 11**, wherein there is further included the step of monitoring for the unauthorized utlization of said system code, and upon discerning unauthorized use, re-initiating programming of said system code of said sensor/transmitter and said central processing unit to change said system code to a new system code.

21. The method of **Claims 1, 2, 3, 4, 7, 8, 9, or 11**, wherein the data is transmitted via radio frequency having a frequency channel, and wherein there is further included the step of monitoring for the unauthorized utlization of said frequency channel. and upon discerning unauthorized use, re-initiating programming of said sensor/transmitters and said central processing unit to a new frequency channel.

22. The method of **Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, or 11** wherein in step "a" of Claim 1, said seed is communicated to said programming device via scanning a bar code.

23. The method of **Claim 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, or 11**, wherein in step "a" of Claim 1, said seed is communicated to said programming device via reading a magnetic strip.

24. The method of **Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, or 11**, wherein said sensor transmitter has programmed power conservation means, said power conservation means for switching said sensor transmitter into a power saving mode, and wherein there is included the additional steps in step "c" of said sensor transmitter waking up upon contacting said programming device, then said sensor transmitter, powering up, handshaking with said programming device, and then being placed into a programming mode to accept programming from said programming device.

25. The method of **Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, or 11**, wherein said sensor transmitter further comprises transmit condition variance means for varying the speed and/or time period of transmission, selective increasing or decreasing the speed of transmission, or selectively transmitting in a continuous mode, burst mode, parcel mode, or other desired transmission rate.

26. The method of **Claim 25**, wherein there is provided the further step of providing self diagnostic means for said sensor transmitter for diagnosing the condition and operability of said sensor transmitter, and there is provided the step of selectively initiating said self diagnostic means, and verifying that said sensor transmitter is functioning within acceptable parameters.

27. The method of programming a sensor transmitter in a secure manner, comprising the steps of:

a. providing a programming device containing sensor transmitter identification and function information comprising programming data bits, said programming device further containing in memory a scrambling algorithm;

b. providing a sensor transmitter containing a scrambling algorithm compatible with said programming device scrambling algorithm;

c. said programming device applying said scrambling algorithm to said programming data bits, producing security/randomization bits which are appended to said programming data bits, forming an outgoing programming message having programming data bits and appended security/randomization bits;

d. transferring said outgoing programming message from said programming device to said sensor transmitter, forming an incoming programming message to said sensor transmitter;

e. said sensor transmitter applying said scrambling algorithm to said incoming data bits in said incoming programming message, providing a scrambling result;

f. comparing said scrambling result to the security/randomization bits appended to said programming data bits in said incoming programming message;

g. upon a correct match of said scrambling result with said security/randomization bits, said sensor transmitter/transmitter accepting said programming data bits in said incoming programming message from said programming device as from a valid, secure programming device, and

h. said sensor transmitter transmitting a verification message verifying valid programming.

28. The method of **Claim 27** whereby the linking of said programming station to said sensor transmitter is accomplished magnetically or optically.

29. The method of **Claim 27**, wherein, following step "g", there is included the additional step of said programming station, once verifying that said sensor transmitter has been successfully programmed, said programming station sending a coded JAM command to said sensor transmitter, said sensor transmitter permanently latching said jam command into a flip-flop in such a manner as to logically disconnect the programming connection for said sensor transmitter so that future incoming programming commands received by said sensor transmitter will be ignored.

30. The method of **Claim 27,** wherein there is provided the additional step in step "c" of said programming station, encrypting said programming data bits, and said sensor transmitter decrypting said programming data bits.

31. The method of **Claim 27**, wherein said security/randomization bits are communicated to said programming device via optical data link, said optical data link further including the steps of reading a bar code.

32. The method of **Claim 27**, wherein said security/randomization bits are communicated to said programming device via reading a magnetic stripe.

33. The method of **Claims 27, 28, 29, 30, 31, or 32**, wherein there is further included the step of monitoring for the unauthorized utlization of said spread spectrum code, and upon discerning unauthorized use, re-initiating programming of said spread spectrum code of said sensor/transmitters and said central processing unit to change said spread spectrum code to an new spread spectrum code.

34. The method of **Claims 27, 28, 29, 30, 31, or 32**. wherein there is further included the step of monitoring for the unauthorized utlization of said system code, and upon discerning unauthorized use, re-initiating programming of said system code of said sensor/transmitters and said central processing unit to change said system code to an new system code.

35. The method of **Claims 27, 28, 29, 30, 31, or 32**, wherein the programming message of step "d" is transferred via radio frequency having a frequency channel, and wherein there is further included the step of monitoring for the unauthorized utlization of said frequency channel, and upon discerning unauthorized use, re-initiating programming of said sensor/transmitters and said central processing unit to a new frequency channel.

36. The method of **Claim 27, 28, 29, 30, 31, or 32**, wherein after step "f" of **Claim 27**, there is included the further step of said sensor transmitter transmitting a verification burst upon completion of programming, said verification burst comprising a digital data string verifying said sensor transmitter's address/ID Code, type code, property code, spread spectrum channel, and seed.

37. The method of **Claim 36**, wherein said verification burst includes a data string indicating status conditions of said sensor transmitter.

38. The method of programming a sensor transmitter in a secure manner, comprising the steps of:

a. providing sensor transmitter identification and function information comprising programming data bits;

b. applying a scrambling algorithm to said programming data bits, producing security/randomization bits, appending said security/randomization bits to said programming data bits, forming a programming message having programming data bits and security/randomization bits;

c. providing a sensor transmitter containing in memory a scrambling algorithm compatible to said scrambling algorithm in step "b";

d. transferring said programming message to said sensor transmitter, forming an incoming programming message to said sensor transmitter;

e. said sensor transmitter applying said scrambling algorithm in said memory to said incoming programming data bits in said incoming programming message, providing a scrambling result;

f. comparing said scrambling result to the security/randomization bits appended to said programming data;

g. upon a correct match of said scrambling result with said security/randomization bits, said sensor transmitter accepting said data bits in said incoming programming message as from a valid, secure programmer, and

h. upon verification of a secure programmer, said sensor transmitter accepting said data from said programming device.

39. The method of **Claim 38**, wherein there is included the further step of said sensor transmitter transmitting a verification burst upon completion of programming, said verification burst

comprising a digital data string verifying said sensor transmitter's address/ID Code, type code, property code, spread spectrum channel, and seed.

40. The method of **Claim 39**, wherein there is included the additional step of verifying said sensor transmitter's programming, and upon verification, transmitting a JAM command addressed to the verified sensor transmitter, said JAM command preventing unauthorized tampering of said verified transmitter.

41. The method of **Claim 38** whereby the linking of said programming station to said sensor transmitter is accomplished magnetically or optically.

42. The method of **Claim 38**, whereby there is further included, after step "g", the additional step of sending a coded JAM command to said sensor transmitter, said sensor transmitter comparing said JAM command with said programming message and, upon verifying a match, said sensor transmitter permanently latching said jam command into a flip-flop in such a manner as to logically disconnect the programming connection so that future incoming programming command will be ignored.

43. The method of **Claim 38**, wherein there is provided the additional step in step "b" of encrypting said programming data bits, and wherein there is provided the additional step in step "e" of said sensor transmitter decrypting said encrypted programming data bits.

44. The method of **Claim 38**, wherein said verification burst includes a sensor transmitter identification code and power status.

45. The method of **Claim 38**, said programming message in step "b" is stored and scanned from a bar code.

46. The method of **Claim 38**, wherein said programming message in step "b" is stored and read from a magnetic strip.

47. The method of **Claim 38**, wherein said programming station is portable.

48. The method of **Claim 38**, wherein said programming station is part of a receiver or control panel.

49. The method of **Claims 39 or 40**, wherein there is further included the step of monitoring for the unauthorized utlization of said spread spectrum code, and upon discerning unauthorized use,

re-initiating programming of said spread spectrum code of said sensor/transmitters and said central processing unit to change said spread spectrum code to an new spread spectrum code.

50. The method of **Claims 39 or 40**, wherein there is further included the step of monitoring for the unauthorized utlization of said system code, and upon discerning unauthorized use, re-initiating programming of said system code of said sensor/transmitters and said central processing unit to change said system code to an new system code.

51. The method of **Claims 38, 39, or 40**, wherein the data is transmitted via radio frequency having a frequency channel, and wherein there is further included the step of monitoring for the unauthorized utlization of said frequency channel, and upon discerning unauthorized use, re-initiating programming of said sensor/transmitters and said central processing unit to a new frequency channel.

52. The method of programming a sensor transmitter in a secure manner, comprising the steps of:

a. providing sensor transmitter identification and function information comprising programming data bits;

b. applying a scrambling algorithm to said programming data bits, producing security/randomization bits, appending said security/randomization bits to said programming data bits, forming a programming message having programming data bits and security/randomization bits;

c. providing a sensor transmitter containing in memory a scrambling algorithm compatible to said scrambling algorithm in step "b";

d. transferring said programming message to said sensor transmitter, forming an incoming programming message to said sensor transmitter;

e. said sensor transmitter applying said scrambling algorithm in said memory to said incoming programming data bits in said incoming programming message, providing a scrambling result;

f. comparing said scrambling result to the security/randomization bits appended to said programming data;

g. upon a correct match of said scrambling result with said security/randomization bits, said transmitter accepting said data bits in said incoming programming message as from a valid, secure programmer.

h. sending a coded JAM command to said sensor transmitter, said sensor transmitter comparing said JAM command with said programming message and, upon verifying a match, said sensor transmitter initiating a means to disconnect the programming connection, preventing further programming of said sensor transmitter.

53. The method of **Claim 52** whereby the linking of said programming station to said sensor transmitter is accomplished magnetically or optically.

54. The method of **claim 52**, whereby said scrambling algorithm may be alterable.

55. The method of **Claim 52**, wherein there is provided the additional step in step "b" of encrypting said programming data bits, and in step "e" said sensor transmitter decrypting said encrypted programming data bits.

56. The method of **Claim 52**, wherein there is included after step "g" the additional step of said transmitter sending a verification burst to the programmer.

57. The method of **Claim 52**, said programming message in step "b" is stored on a bar code.

58. The method of **Claim 52**, wherein said identification and function information in step "a" is stored on a magnetic strip.

59. The method of **Claim 52**, wherein said programming station is portable.

60. The method of **Claim 52**, wherein said programming station is part of a control panel.

61. The method of **Claim 52**, wherein there is included the further step of said sensor transmitter transmitting a verification burst upon completion of programming, said verification burst comprising a digital data string verifying said sensor transmitter's address/ID Code, type code, property code, spread spectrum channel, and seed.

62. The method of **Claim 61**, wherein there is further included the step of monitoring for the unauthorized utlization of said spread spectrum code, and upon discerning unauthorized use, re-initiating programming of said spread spectrum code of said sensor/transmitters and said central processing unit to change said spread spectrum code to an new spread spectrum code.

63. The method of **Claim 61**, wherein there is further included the step of monitoring for the unauthorized utlization of said system code, and upon discerning unauthorized use, re-initiating programming of said system code of said sensor/transmitters and said central processing unit to change said system code to an new system code.

64. The method of **Claims 52, 53, 54, 55, 56, 57, 58, 59, 60, or 61**, wherein the data is

transmitted via radio frequency having a frequency channel, and wherein there is further included the step of monitoring for the unauthorized utlization of said frequency channel, and upon discerning unauthorized use, re-initiating programming of said sensor/transmitters and said central processing unit to a new frequency channel.

65. A method of programming a sensor transmitter in a secure fashion, comprising the steps of:

a. placing an unprogrammed sensor transmitter in near proximity to an unprogrammed system receiver/panel/programming device;

b. said receiver set into a mode by which it can accept programming data via transmitted programming message from said sensor transmitter;

c. limiting the signal strength of said sensor transmitter to a near proximity of the receiver;

d. selectively generating security/randomization bits for said sensor transmitter, and transmitting said bits to said receiver;

e. said receiver imputing programming message and determining if such a device ID/address already exists in the system;

f. if said new device ID/address is acceptable it becomes internally associated by the system receiver/panel/programming device with said sensor transmitter;

g. if the new device ID/address is not acceptable the receiver or system receiver/panel/programming device so makes an appropriate indication;

h. steps d-g are repeated until step h is met, once met the transmitter is removed from the programming mode.

66. The method of programming a sensor transmitter/transmitter of **Step 65**, wherein after step "g" there is provided the additional step of said receiver inputting said transmission and appending said security/randomization bit to programming data including new device ID/address, forming a programming message, and sending said programming message to said transmitter;

67. The method of programming a sensor transmitter/transmitter of **Step 65** wherein in step "d" there is included the extra step of providing input means for externally inputting said security/randomization bit.

68. The method of programming a sensor transmitter/transmitter of **Claim 65** wherein, once the device ID/address is programmed with the transmitter, said programming button for generating said random number generator feature is configured to reprogram to allow said switch to be utilized to program the spread spectrum code or frequency channel or the like, by depressing said button in increments for selecting the desired channel.

69. The method of programming a sensor transmitter/transmitter of **Claim 65,** wherein there is provided the additional step of the transmitter type code is transferred from the transmitter to said receiver for programming of said receiver.

70. The method of **Claim 65**, wherein there is included the further step of said sensor transmitter transmitting a verification burst upon completion of programming, said verification burst comprising a digital data string verifying said sensor transmitter's address/ID Code, type code, property code, spread spectrum channel, and seed.

71. The method of **Claim 70**, wherein there is further included the step of monitoring for the unauthorized utlization of said spread spectrum code, and upon discerning unauthorized use, re-initiating programming of said spread spectrum code of said sensor/transmitters and said central processing unit to change said spread spectrum code to an new spread spectrum code.

72. The method of **Claim 70**, wherein there is further included the step of monitoring for the unauthorized utlization of said system code, and upon discerning unauthorized use, re-initiating programming of said system code of said sensor/transmitters and said central processing unit to change said system code to an new system code.

73. The method of **Claims 65, 66, 67, 68, 69, or 70**, wherein the data is transmitted via radio frequency having a frequency channel, and wherein there is further included the step of monitoring for the unauthorized utlization of said frequency channel, and upon discerning unauthorized use, re-initiating programming of said sensor/transmitters and said central processing unit to a new frequency channel.

74. The method of programming an array of sensor transmitters to communicate with a central processing unit in a secure fashion, comprising the steps of:

a. providing a EEROM power means for selectively switching power to a sensor transmitter EEROM, limiting the operation of said EEROM to predetermined periods;

b. placing a programming device in a programming mode;

c. placing said sensor transmitter into a mode by which it can accept data via transmitted programming information from said programming device;

d. utilizing said EEROM power means to switch on programming power to said sensor transmitter EEROM, placing said EEROM in a programming mode

e. transmitting programming data from said programming device to said transmitter as part of a programming message;

f. said sensor transmitter inputting said programming message and saving said

programming data in memory;

g. once programming ceases, utilizing said EEROM power means for switching off designated programming power to said EEROM, thereby conserving power.

h. repeating steps b-h until all of said sensor transmitters in said array have been programmed.

75. The method of **Claim 74** wherein there is included the further step of redundantly saving said seed and programming data in said EEROM, thereby providing a backup of said programming data upon corruption of part of the memory of said sensor transmitter, said EEROM further comprising error detection means for detecting errors in data stored in memory.

76. The method of **Claim 75**, wherein said EEROM power means comprises a logic cage whose logic high output is capable of conveying sufficient power to the EEROM.

77. The method of **Claim 75**, wherein said EEROM power means comprises a pass transistor in series with the EEROM's Ucc power lead.

78. The method of **Claim 75, 76, or 77**, wherein there is provided the additional step of providing EEROM limited programming means for limiting programming of said EEROM to that period when said programming device is providing power to said sensor transmitter.

79. The method of **Claims 74, 75, 76, or 77,** wherein said sensor transmitter has programmed therein power conservation means, said power conservation means for switching said sensor transmitter into a power saving mode, and wherein there is included the additional steps in step "c" of said sensor transmitter waking up upon contacting said programming device, then said sensor transmitter, powering up, handshaking with said programming device, and then being placed into a programming mode to accept programming from said programming device.

80. The method of **Claims 74, 75, 76, or 77**, wherein said programming device transmits data to said sensor transmitter utilizing a magnetic loop/induction system, and is configured only to initiate programming sequence only upon exposure to a magnetic field exceeding a predetermined field strength, generated by said magnetic loop/induction system.

81. The method of **Claim 80**, wherein said sensor transmitter is configured to utilize said magnetic field generated by said magnetic loop/induction system to power said sensor transmitter.

82. The method of **Claim 74, 75, or 76**, wherein after step "f" of **Claim 74**, there is

included the further step of said sensor transmitter transmitting a verification burst upon completion of programming, said verification burst verifying correct programming of said sensor transmitter.

83. The method of **Claim 82** wherein there is included the additional step of verifying said sensor transmitter's programming via said verification burst, and upon verification, transmitting a JAM command addressed to the verified sensor transmitter, said JAM command altering the programmability of said sensor transmitter, preventing unauthorized programming or tampering of said verified transmitter.

84. The method of programming an array of sensor transmitters to communicate with a central processing unit in a secure fashion, comprising the steps of:

a. providing a programming device having an magnetic loop coil;

b. placing a programming device in a programming mode;

c. providing a sensor transmitter with power conservation means, said power conservation means including a low power mode and a high power mode, and switching means for switching from a lower power mode to a high power mode, and visa-versa, said sensor transmitter further having magnetic field sensing means for sensing a predesignated magnetic field;

d. setting said magnetic loop coil to emit a predesignated magnetic field strength, and placing said magnetic loop coil into the reception range of said magnetic field sensing means;

e. upon sensing a predesignated magnetic field, said magnetic field sensing means switching said power conservation means from a low power mode to a high power mode, placing said sensor transmitter into a mode by which it can accept data via transmitted programming information from said programming device;

f. transmitting programming data from said programming device to said transmitter as part of a programming message;

g. said sensor transmitter inputting said programming message and saving said programming data in memory;

h. once programming ceases, utilizing said power conservation means for switching said sensor to a lower power mode, thereby conserving power.

i. repeating steps b-h until all of said sensor transmitters in said array have been programmed.

85. The method of **Claim 84**, wherein there is provided the additional step of said sensor transmitter utilize said magnetic field generated by said magnetic loop/induction system to power said sensor transmitter.

86. The method of **Claim 84**, wherein after step "g" of **Claim 1**, there is included the

further step of said sensor transmitter transmitting a verification burst upon completion of programming, said verification burst verifying correct programming of said sensor transmitter.

87. The method of **Claim 86**, wherein there is included the additional step of verifying said sensor transmitter's programming via said verification burst, and upon verification, transmitting a JAM command addressed to the verified sensor transmitter, said JAM command altering the programmability of said sensor transmitter, preventing unauthorized programming or tampering of said verified transmitter.

88. The method of **Claims 84, 85, 86, or 87**, wherein said sensor transmitter further comprises transmit condition variance means for varying the speed and/or time period of transmission, and wherein there is further included the step of selectively varying the speed of transmission or selectiively transmitting in a continuous mode, burst mode, parcel mode, or other desired transmission rate.

89. The method of **Claims 84, 85, 86, or 87**, wherein said sensor transmitter further comprises transmit condition variance means for varying the speed and/or time period of transmission, and wherein there is further included the step of selectiively transmitting in a continuous mode, burst mode, or parcel mode.

90. The method of **Claim 84**, wherein there is provided the further step of providing self diagnostic means for said sensor transmitter for diagnosing the condition and operability of said sensor transmitter, and there is provided the step of selectively initiating said self diagnostic means, and verifying that said sensor transmitter is functioning within acceptable parameters.

91. The method of programming an array of sensor transmitters to communicate with a central processing unit in a secure fashion, comprising the steps of:

a. providing a programming device having an optical data link;

b. placing a programming device in a programming mode;

c. providing a sensor transmitter with power conservation means, said power conservation means including a low power mode and a high power mode, and switching means for switching from a lower power mode to a high power mode, and visa-versa, said sensor transmitter further having an optical input and optical sensing means for sensing a optical emission;

d. setting said optical data link of said programming device to emit a predesignated optical emission, and placing said optical input of said sensor into the reception range of said optical data link;

e. upon sensing a predesignated optical emission, said optical sensing means switching

said power conservation means from a low power mode to a high power mode, placing said sensor transmitter into a mode by which it can accept data via transmitted programming information from said programming device;

f. transmitting programming data from said programming device to said transmitter as part of a programming message;

g. said sensor transmitter inputting said programming message and saving said programming data in memory;

h. once programming ceases, utilizing said power conservation means for switching said sensor to a lower power mode, thereby conserving power.

i. repeating steps b-h until all of said sensor transmitters in said array have been programmed.

92. The method of **Claim 91**, wherein there is provided the additional step of said sensor transmitter utilizing said optical emission generated by said optical data link power said sensor transmitter.

93. The method of **Claim 91**, wherein after step "g" of **Claim 91**, there is included the further step of said sensor transmitter transmitting a verification burst upon completion of programming, said verification burst verifying correct programming of said sensor transmitter.

94. The method of **Claim 93**, wherein there is included the additional step of verifying said sensor transmitter's programming via said verification burst, and upon verification, transmitting a JAM command addressed to the verified sensor transmitter, said JAM command altering the programmability of said sensor transmitter, preventing unauthorized programming or tampering of said verified transmitter.

95. The method of **Claims 91, 92, 93, or 94**, wherein said sensor transmitter further comprises transmit condition variance means for varying the speed of transmission, and there is included the additional step of selectively varying the speed of transmission.

96. The method of **Claims 91, 92, 93, or 94**, wherein said sensor transmitter further comprises transmit condition variance means for varying the time period of transmission, and wherein there is included the step of selectively transmitting in a continuous mode, burst mode, parcel mode, or other desired transmission rate.

97. The method of **Claim 96**, wherein there is provided the further step of providing self diagnostic means for said sensor transmitter for diagnosing the condition and operability of said sensor

transmitter, and there is provided the step of selectively initiating said self diagnostic means, and verifying that said sensor transmitter is functioning within acceptable parameters.

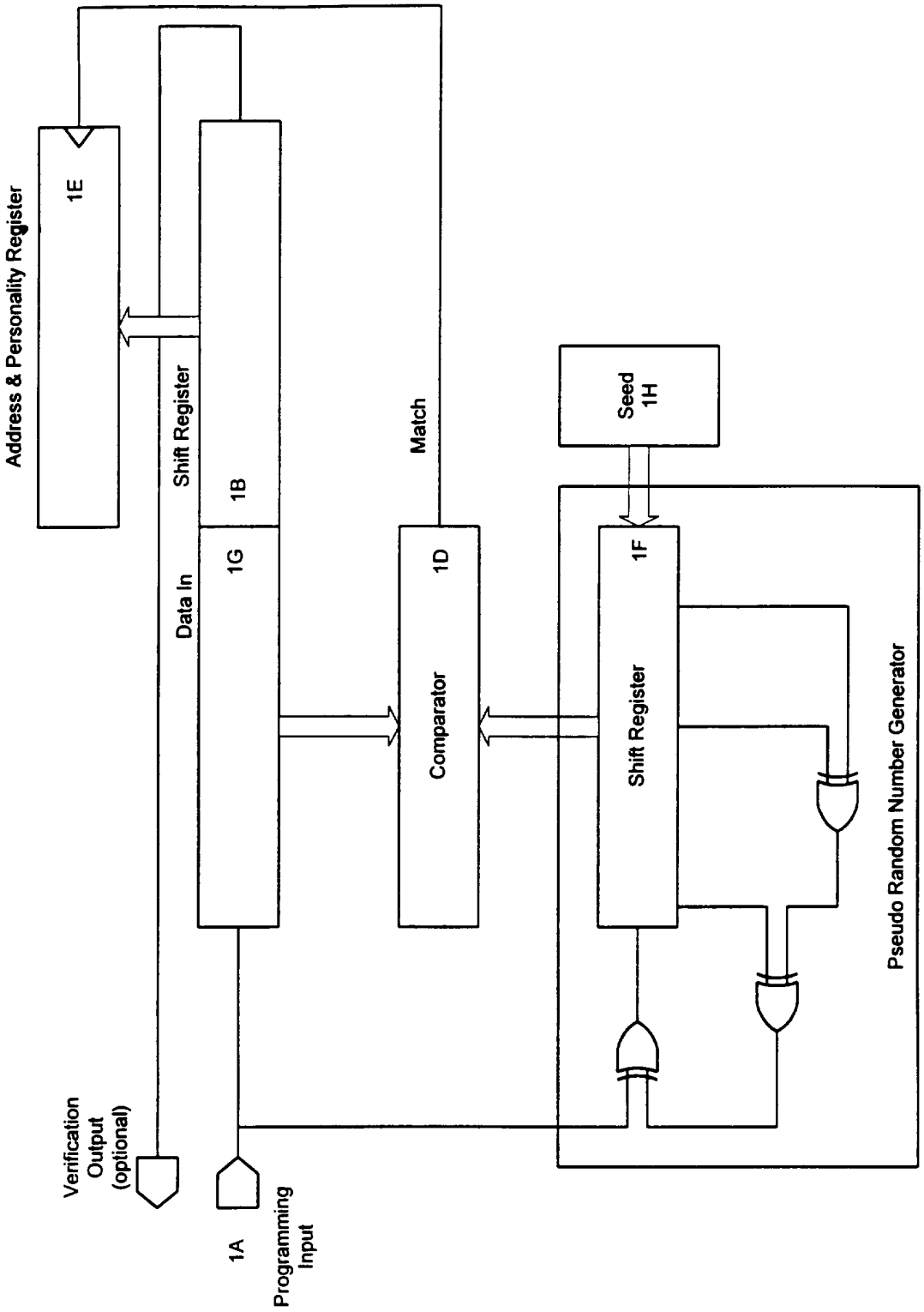


FIGURE 1

RECTIFIED SHEET (RULE 91)

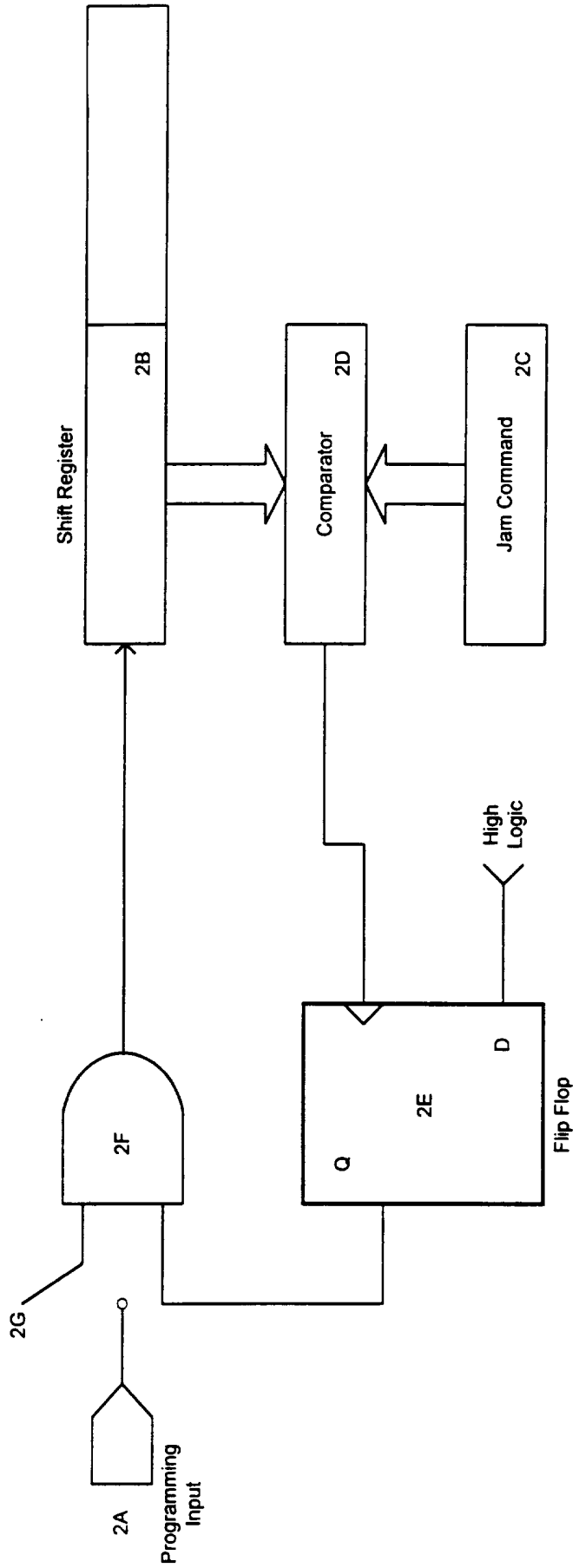


FIGURE 2

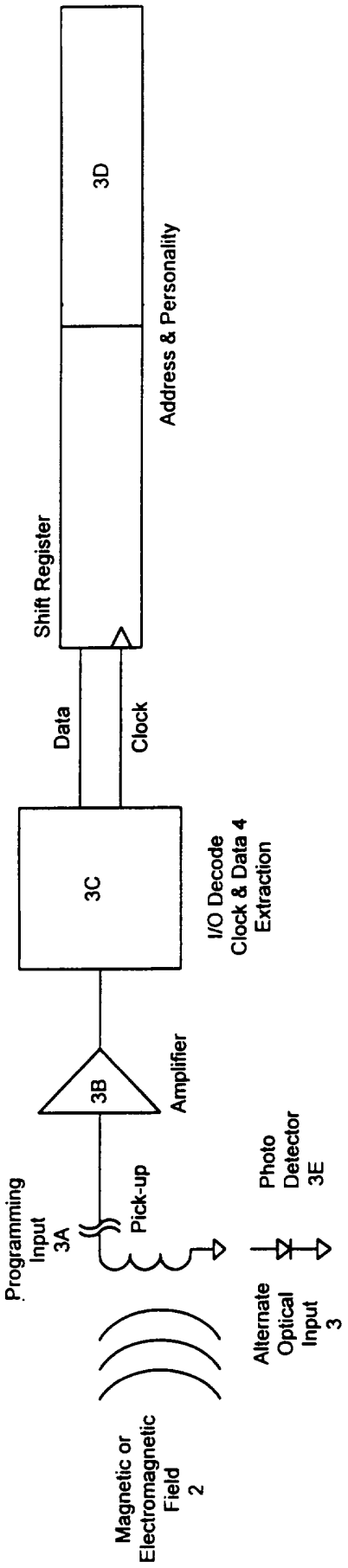


FIGURE 3

RECTIFIED SHEET (RULE 91)

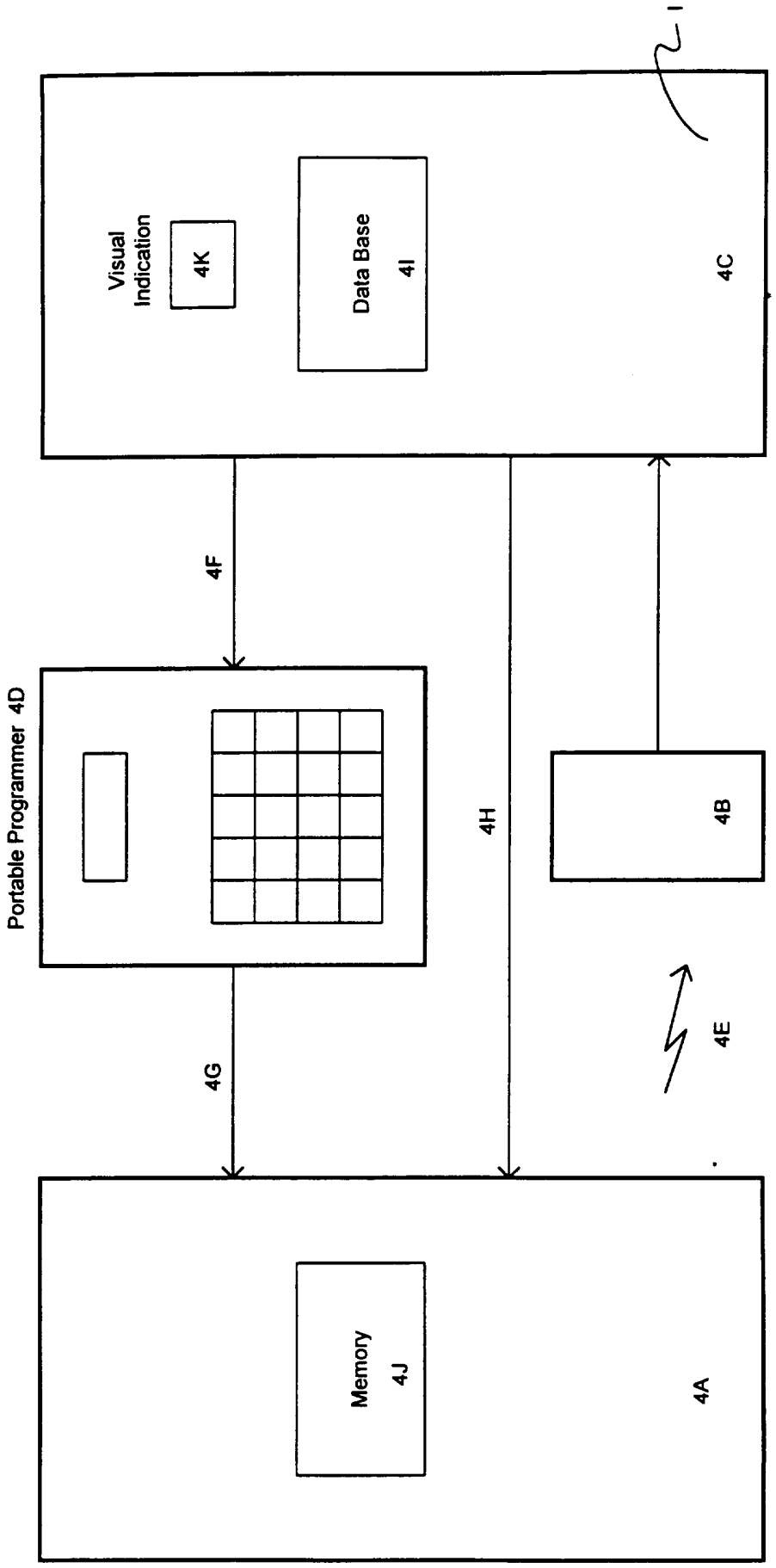


FIGURE 4

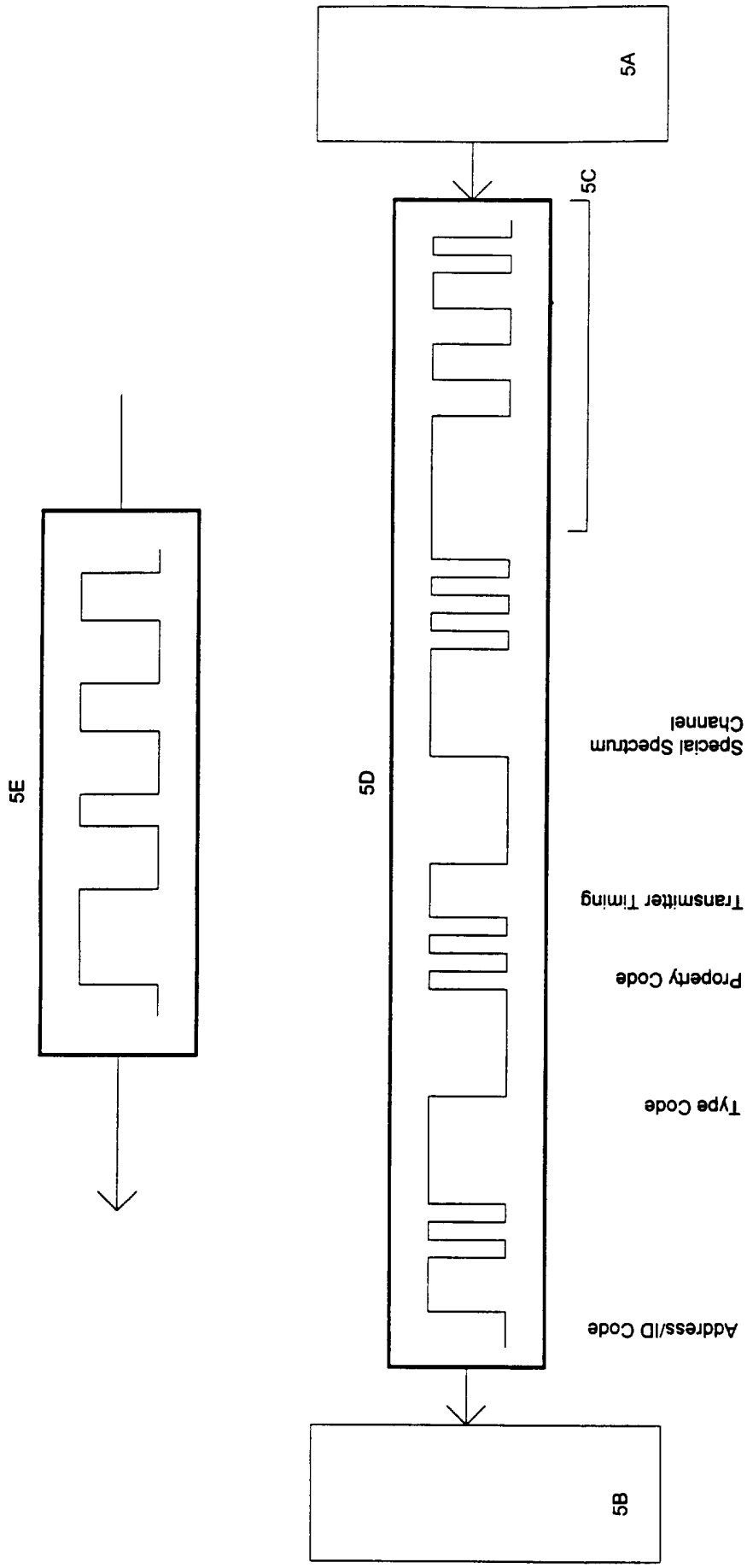


FIGURE 5

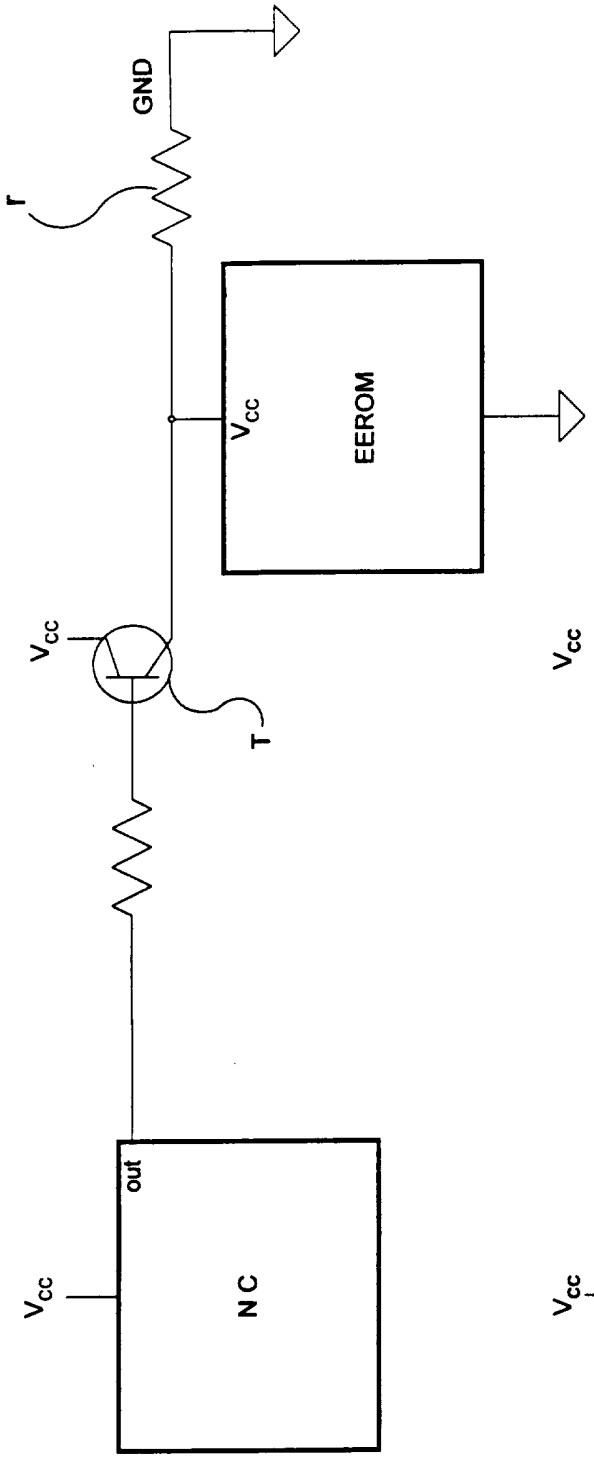


FIG. 6A

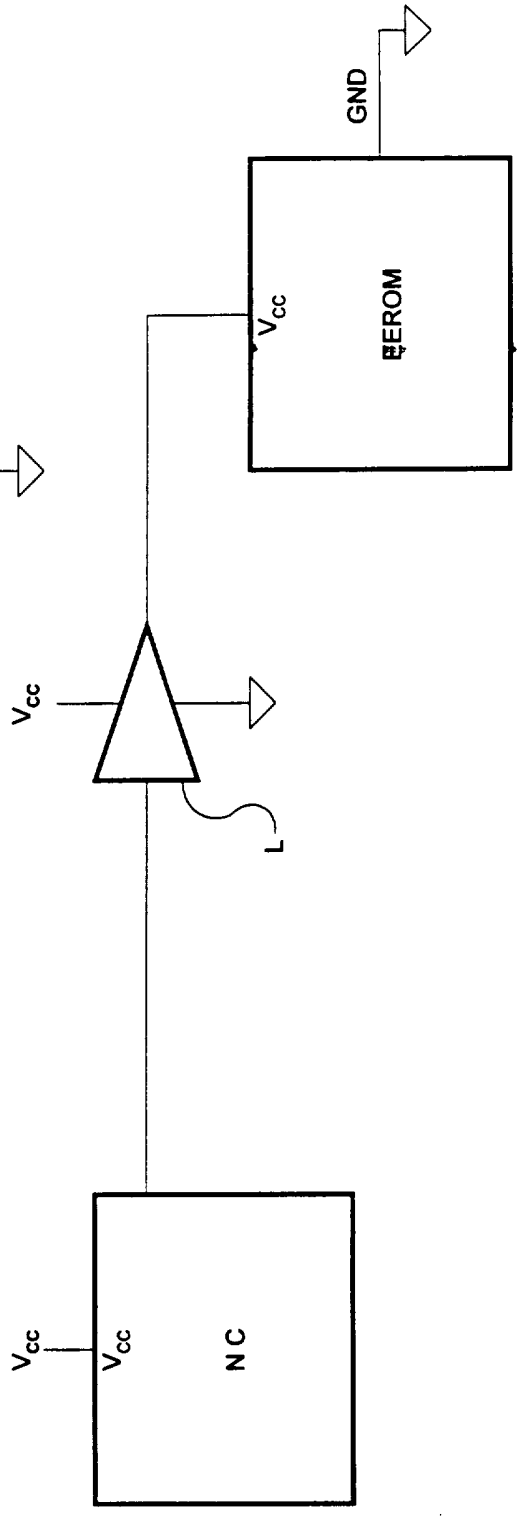


FIG. 6B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/04731

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G08B 29/00; H04L 9/00
US CL :340/506
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 340/505, 506, 517, 518, 539, 825.06, 825.22, 825.31, 825.5, 825.69, 825.72; 375/200; 380/4, 9, 236/51; 342/51; 385/4, 57

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 4,737,770 (BRUNIUS ET AL) 12 April 1988, see Figs. 2, 5 and 6.	1, 2, 65-70, 73, 87
Y	US, A, 4,772,876 (LAUD) 20 September 1988, see col. 1, lines 50-65.	1, 2, 65-70, 73, 87
A	US, A, 4,847,577 (GERHART ET AL) 11 July 1989, see Figs. 6 and 7.	1, 2, 65-70, 73, 87
Y	US, A, 5,302,941 (BERUBE) 12 April 1994, see Fig. 1. and col. 4.	1, 2, 65-70, 73, 87
Y, E	US, A, 5,408,217 (SANDERFORD, JR) 18 April 1995, see entire document.	1-3, 27-33, 38-49, 52-78, 84-88, 90-95

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be part of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
01 AUGUST 1995

Date of mailing of the international search report
15 SEP 1995

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
SALVATORE CANGIALOSI
Telephone No. (703) 308-0482

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/04731

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 5,259,029 (DUNCAN, JR) 02 November 1993 ,see entire document.	1, 2, 65-70, 73, 87
Y	US, A, 5,396,541 (FARWELL ET AL) 07 March 1995, see Fig. 5.	1, 2, 3, 65-71, 73, 87
Y	US, A, 4,977,577 (ARTHUR ET AL) 11 December 1990, see Figs. 1 and 2.	3, 71
Y	US, A, 5,341,988 (REIN ET AL) 30 August 1994, see Figs. 6-9.	3, 71
Y	US, A, 4,831, 438 (BELLMAN, JR. ET AL) 16 May 1989, see element 121 and col. 6, lines 25-50.	27-33, 38-49, 52-64, 74-78
Y	US, A, 4,952,817 (BOLAN ET AL) 28 August 1990 ,see Figs 1, 2 and 6.	84-86, 88, 90-95
Y	US, A, 5,305,008 (TURNER ET AL) 19 April 1994, see Figs. 8 and 12.	84-86, 88, 90
Y	US, A, 4,903,340 (SORENSON) 20 February 1990, see Fig. 2.	90-95
Y	US, A, 5,268,980 (YUUKI) 07 December 1993, see Fig. 1.	90-95

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/04731

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☒ Claims Nos.: 4-26, 34-37, 50-51, 79-83, 89, 96, 97
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/04731

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING
This ISA found multiple inventions as follows:

Group I, Claims 1, 2, 65-70, 72, 73 and 87, drawn to a method of validating programming in a sensor array.
Group II, Claims 3 and 71, drawn to a method of using spread spectrum in a sensor array.
Group III, Claims 27-33, 38-49 and 52-64 drawn to method of using a scrambling algorithm in a sensor array.
Group IV, Claims 74-78 drawn to method of using an EPROMING sensor array.
Group V, Claims 84-86, 88 and 90 drawn to a method of using a magnetic field sensor.
Group VI, Claims 90-95, drawn to a method of using an optical coupling in a sensor array.

The inventions listed as Groups I-VI do not relate to a single inventive concept under PCT Rule 13.1, because under PCT Rule 13.2, they lack the same or corresponding technical features for the following reasons: The inventions of Groups II-VI lack the technical features of validation and selective seed choice. The inventions of Groups I, III-VI lack the technical features of spread spectrum. The inventions of Groups I, II, IV-VI lack the technical feature of a scrambling algorithm. The inventions of Groups I-III, V, VI lack the technical feature of an EPROM. The inventions of Groups I-IV, and VI lack the technical feature of a magnetic sensor.
The inventions of Groups I-V lack the technical feature of an optical coupling.