Title: CELLULAR COMMUNICATION DEVICE-BASED ANTI-THEFT/ANTI-INTRUSION WARNING AND CONTROL SYSTEM

Abstract: An anti-theft/anti-intrusion warning and control system capable of notifying, in real-time, owners and other interested parties of protected vehicles, private movable property, and protected areas, of a security threat to their property involving theft or intrusion. The warning and control system provides for remote monitoring and reporting of protected property utilizing strategically placed sensors and a cellular communications device which communicates information via a telecommunications network to the owners and other interested parties of the status of their property. The cellular communications device enables remote operation and control of selected devices, components, and systems associated with a protected property and provides for remotely actuating countermeasures to thwart security threats.
For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
CELLULAR COMMUNICATIONS DEVICE-BASED
ANTI-THEFT/ANTI-INTRUSION WARNING AND CONTROL SYSTEM

FIELD OF THE INVENTION

The present invention generally relates to a cellular communications device-based anti-theft/anti-intrusion security system, and more particularly, to an anti-theft/anti-intrusion warning and control system providing real-time notification, and remote implementation of countermeasures to thwart unauthorized intrusion into protected areas and to remotely control anti-theft/anti-intrusion devices for vehicles and other movable property utilizing a cellular communications device.

BACKGROUND OF THE INVENTION

Anti-theft/anti-intrusion systems are most prominent in vehicles, homes, offices, and commercial premises, but most such systems, whether passive alarms, such as flashing lights or sirens, or active devices, such as automatically operated door locks, are susceptible to being disabled by skilled thieves.

One of the most significant problems with systems designed to locate stolen vehicles, for example, is that once the vehicle is reported stolen, the system response time is critical for achieving a successful vehicle retrieval rate. Often, the vehicle owner is not aware of the theft immediately, and the vehicle is reported stolen only several hours after the theft, when it becomes apparent to the owner. might not be notified until hours after the event when it is too late to implement further anti-theft/anti-intrusion security measures if these are not already in place prior to the notification of the event.

Furthermore, most of the available vehicle location systems are very expensive to install, and therefore, only the most expensive cars are protected. In some cases, these cars are company-owned vehicles, so that the burden of the expense falls on the company, and not on the vehicle’s user. This situation leads to a large proportion of unprotected vehicles, available for theft without effective deterrence.

In addition, many homes, offices, and commercial premises remain unused for many hours of the night and on weekends and offer temptation for unauthorized intrusion and theft of valuable property. Standard alarm systems, such as those which use audio alarms, flashing lights, and the
like, are limited to warning of unauthorized access, but do not attempt, in most cases to actively
thwart intruders. When silent burglar alarms are transmitted, for example, to a security service or to
the police, response time may not be effective in preventing the escape of the intruders. The owners
might not be notified until hours after the event when it is too late to implement further anti-theft/
anti-intrusion, security measures if these are not already in place prior to notification of the event.

SUMMARY OF THE INVENTION

Accordingly, it is a principal object of the present invention to overcome the disadvantages
of prior art anti-theft/anti-intrusion protection systems, and provide an anti-theft/anti-intrusion
warning and control system capable of notifying, in real-time, owners of vehicles, homes, offices,
business premises, industrial sites, and fenced-in areas such as farmland, grazing areas, and private
estates of a security threat to their property, and enabling monitoring and remote control of devices,
components, systems — as well as parts of devices, components, and systems — to thwart such
security threats.

Therefore, there is provided an anti-theft/anti-intrusion warning and control system
comprising a sensor input unit for reporting information about the status of at least one of a sensor-
protected property and area; a sensor detector unit for monitoring and reporting information
received from the sensor input unit; a cellular transceiver for communicating over a
telecommunications network; an auto-dialer/tone generator unit for dialing at least one pre-
programmed telephone number and generating a warning tone via the transceiver in response to
detection of a security threat; a memory unit connected to the auto-dialer for storing the at least one
pre-programmed phone number for the auto-dialer to access and dial; at least one user interface for
inputting at least one secret user code to access the warning and control system; a dual-tone, multi-
frequency (DTMF) detector unit for decoding tones received by the transceiver into the at least one
user code; a code detector/processor unit for comparing the at least one user code with at least one
pre-programmed code stored in the warning and control system; an alarm unit for activating at least
one alarm and arming at least one anti-theft/anti-intrusion security measure associated with at least
one of a protected property and a protected area in accordance with the code detector/processor unit
comparison of the at least one user code and the at least one pre-programmed code; and an output
unit for executing the at least one anti-theft/anti-intrusion security measure.

It is another object of the invention to provide an anti-theft/anti-intrusion warning and
control system further comprising: a battery back-up unit to provide emergency electrical service to
the warning and control system independently of any existing electrical service associated with the
at least one of protected property and protected area; and an emergency alarm switch for communicating an alarm signal directly to the at least one authorized receiver, while simultaneously activating pre-programmed at least one anti-theft/anti-intrusion security measure.

It is yet another object of the invention to provide a warning and control method comprising the steps of initializing the warning and control system status; monitoring at least one of a vehicle, a protected property, and a protected area; detecting a security threat to at least one of the vehicle, protected property, and protected area; activating an alarm to notify others of the security threat; establishing at least one communications link over a telecommunication network to at least one authorized receiver of the security threat notice; sending a first secret code response back to the warning and control system from the at least one authorized receiver; utilizing a first secret code to activate at least one security measure provided by the warning and control system to thwart the imminent security threat; sending a second secret code to the warning and control system to return the warning and control system to Standby mode after the current security threat has been counteracted; and communicating additional secret codes to the warning and control system to monitor and operate selected devices, functions, and systems affecting the general operation and security of the at least one of a protected vehicle, a protected property, and a protected area.

It is important to note that the term “security threat”, as used herein, is any physical threat to protected property arising from unauthorized entry into private, protected areas, and theft of protected property, both real property and personal property.

The term a “protected area”, as defined herein, is a designated area whose perimeter is marked by a fence or similar border marking, so as to guard and thwart security threats. Examples of protected areas include: estates of private homes, business premises, agricultural land, industrial or military compounds, and the like.

The term “vehicle” as used herein, is any conveyance for carrying or conveying persons or objects over, on, or under land, sea, or air – including, but not limited to – an automobile, a truck, a bus, a tractor-trailer, a railroad car, an electric forklift, a cement-mixer, a fire-engine, a snowmobile, a motorcycle, a mobile home, a home trailer, a marine vessel, a ship, a boat, a submarine, an aircraft, a jet plane, a dirigible, a blimp, a satellite, a rocket, and any type of mobile agricultural and construction equipment.

In the case of a vehicle, it is protected against theft when the doors are closed and the system is set to Standby mode by the remote system activation controller, typically a hand-held remote activation device widely used today for this purpose. When a “legal” entry is made into the vehicle, the vehicle user must enter, within about 20-30 seconds of the entry, a secret code into a
user interface, such as a keypad or a fingerprint reader. This action cancels activation of the protection system.

When an "illegal" entry is made into a vehicle, the system is activated via sensors or by the door frame switch which detects the door opening, or by similar switches mounted on windows and other points of the vehicle normally accessed, such as an engine hood, a trunk cover, a cabin hatch, a storage compartment, a fuel or water compartment cover, and the like. The sensors or switches enable the detection of a breach in the integrity of the openings.

When an "illegal" entry has been detected, the system establishes communication in real-time with the vehicle owner via a cellular communications device by dialing directly to his personal cellular phone, or to one or more pre-programmed telephone numbers, such as a security service, police, etc., over standard telephone communication lines and begins arming the anti-theft/anti-intrusion devices of the system. Communications are simultaneously enabled to all contacts pre-programmed to be notified of a theft in progress or an intrusion.

Once communication has been established, the system provides notification of the illegal entry to the vehicle, such as by playing an appropriate pre-recorded message, or transmitting an alarm-type sound signaling a breach of security. The owner or other authorized security person hearing the message or alarm signal then dials a secret code on his cellular or touch-tone telephone, which activates one or more security devices or systems in or on the vehicle to remotely monitor and/or control one or more systems, subsystems, devices, and components, of the vehicle. Monitoring is provided by hidden microphones and/or video cameras for live audio or video transmission and optional, remote recording and playback. Control systems, devices, and components usually activated are those which can immobilize or disable the vehicle when not activated or disconnected, or those, such as headlights, running lights, sirens, or horns, which call unwanted attention to the object of an attempted theft or intrusion.

It is also possible to restore the vehicle to the Standby mode by remote control by dialing an appropriate secret code.

If there is no response by the vehicle owner when the warning and control system of the invention attempts to establish communication, another telephone number stored in the autodialer memory may be downloaded for a second attempt to place a call, or a third attempt may be made if the first and second attempts have not succeeded. This is a sequenced warning method based on the importance or priority given to designated individuals, such as an owner, in dealing with a security threat.

In the event that there is no communication established with any of the pre-programmed priority telephone numbers, the anti-theft/anti-intrusion system is programmable to operate
autonomously and dials a first designated number, for example, the police or a security service who are authorized by an owner to deal with a security threat situation. If no answer, or unable to complete a call, the program downloads a second phone number from the autodialer memory and dials it. A third phone number is programmed to be dialed in the event the second number fails to elicit a coded response.

The phone numbers dialed, in an alternate embodiment, are dialed simultaneously to notify all authorized parties of a security threat, rather than using sequential dialing and individual notification, which is a slower method of getting action and responding to a security threat.

Several warning functions may be automatically activated together for a greater deterrent effect. Also, the alert call may be in the form of a signal or tone, or a pre-recorded warning message stored in the auto-dialer/tone generator’s memory. In an automobile, this may include causing the brake lights to flash, together or without flashing rear back-up lights, and/or front-fender lights. After a certain predetermined interval, the vehicle is shut down by de-activating other vital control functions, such as the fuel injection system, the hydraulic system, or mechanical features necessary for the operation of the vehicle.

When the vehicle is stolen from an area in which there is no reception of cellular telephone communications, the system “remembers” that there was an illegal entry, and when the vehicle reaches an area capable of cellular telephone communications, the system redials the pre-programmed phone numbers to establish communication. Even in an area where there are no cellular telephone communications, the secret code must be entered to avoid having the system activated, and the activation is also possible even when the vehicle’s battery is disconnected during the illegal entry.

When a vehicle is serviced at a garage, entry of an additional secret code in the vehicle’s keypad, known only to the vehicle owner and the garage owner or manager, disables the vehicle’s system entirely, and its operation can only be restored by entry of the secret code for system activation. Thus a service garage can effectively prevent theft of vehicles from his premises while a vehicle is waiting for service on a garage lot or left unattended for any lengthy period of time.

It is not necessary to rely on the automatic dialing function of the invention normally activated upon an illegal entry or attempted theft of a vehicle. It is possible to establish communication with a vehicle and achieve the remote control and/or monitoring functions at any time by dialing over any standard wired or wireless telecommunications network using a touch-tone keypad. Wired, wireless, cordless, as well as cellular telephones can be used for this purpose. A PC or other modem-enabled, networked device is another option to utilize with the inventive system. Telecommunications can be established simultaneously with the inventive system over one
or more varieties of networks, such as telephony, telegraphy, cellular, and the like, and using different communications devices.

The inventive warning and control system enables the vehicle's owner to be actively involved in protecting the vehicle from theft, and enhances enforcement activities at the local level. The response time for police and emergency personnel is reduced by early notification of the vehicle theft, reducing the overall waiting time associated with prior art location systems.

The system has additional advantages since it may actually reduce personal injuries inflicted by thieves, if, for example, a vehicle is forcibly taken from a driver, in a hijacking situation. The vehicle owner may be less concerned with releasing the vehicle to the thief, knowing it is equipped with the inventive system, allowing the vehicle owner to have remote control of vehicle functions and monitoring in real-time of the event.

An optional feature of the invention is an emergency alarm switch which provides rapid notification of a security threat via the cellular communications device if an owner of a vehicle, for example, is aware of an imminent security threat. Although such switches are commonly used by bank tellers to silently alert security personnel or police that a robbery is in progress, they do not control countermeasures to thwart robbery, but only alert and summon security personnel. The present invention improves on this role, by enabling implementation of countermeasures simultaneously to giving a warning alarm. Taxis and other public conveyances with high risk for drivers are enabled to automatically establish communication with their dispatchers or with other desired emergency contacts and also implement pre-programmed countermeasures. The distress button generates a telecommunications signal transmitted directly to a remote party, easily identified as an alarm and alerting those contacted of a security problem.

Another feature of the invention is the provision of a hidden secret code known only to a service company which is authorized by the user. This hidden code serves to replace the code normally provided by the user, in the case where the user has forgotten his code, or in the case that the secret code has become known to unauthorized users. In this fashion, the warning and control system operation is further protected against unauthorized use.

In an alternative embodiment, the inventive warning and control system is also applicable to other environments, such as protected premises and fenced-in areas. With appropriate modification, the system can be powered by a battery charger and hidden battery back-up system. A set of sensors, such as door and window entry sensors, can be supplied and connected by direct wiring or by wireless connection, such that the system is not dependent on existing telephone or electrical systems.
The sensors detect an illegal entry, and the inventive system operates to establish communication with the subscriber to the services of the inventive system, such as a home or business owner, or alternatively, with two different pre-selected telephone numbers. The communication is accomplished by a telephone call placed over wireless, cellular communications, to a cellular telephone or wired telephone line. Upon answering the call, the subscriber receives a pre-recorded audio message, either by synthesized voice or by a warning siren, that there is an illegal entry. By entry of a secret code, the subscriber can operate a hidden, remote control camera, which can be connected to a hidden video recorder, to record the illegal activity. Optionally, the video camera can transmit the images to a remote recorder and/or monitor over a wide band telecommunications transmission system. The monitor enables viewing in real time. By use of appropriate hidden microphones, it is possible for the subscriber to hear the activity taking place on the premises. The remote control function also enable disconnection of the system.

Further anti-theft/anti-intrusion security measures comprise the use of personal defense aerosols and/or sprays which, when operated remotely, actively deter would-be thieves and/or intruders. Tear gas and other disabling gases may be used in special cases, such as protection of official government or military premises, vehicles, or protected, fenced-in areas.

The warning and control system can also be operated to enable communication initiated by an owner via cellular telephone connection, or by wired telephone line connection. Once connected, the system enables controlled operation of the hidden camera, or operation of accessories such as an air conditioner, or other electrical devices, such as lights.

The cellular communication device conveniently enables a property owner to remotely access and communicate with the warning and control system through the use of a special secret code known only to the owner, similar in practice to the method of accessing an account at an ATM for after-hour banking, and well known to those skilled in the art. Special secret codes are provided for making remote changes in the programs associated with any parts of the warning and control system. The telephone numbers stored in the memory unit, the pre-programmed code commands for control functions, and the secret codes themselves, are also managed remotely, and can be changed, deleted, or edited as needed.

In one embodiment, for example, to replace a pre-programmed telephone number in the memory unit, the owner dials into the warning and control system using a cellular communication device, such as a cellular phone, enters a special code enabling access to designated tasks (manage phone list), presses a single "hot" key identifying the specific action to be taken (replace a phone number), dials the old phone number to be replaced (or selects the phone number from a scroll list), presses a second "hot" key to delete the old phone number, keys-in the new phone number and
presses another "hot" key to save the new number into memory, listens for an automatic confirmation signal that the task has been completed, and hangs up. The next time the warning and control system searches for a telephone number, the replacement number will be available for use.

Alternatively, management functions for the warning and control system can be displayed on a screen on the cellular communication device, either called up by dialing a designated short phone number, or downloaded over the phone network from the warning and control system database. Editing can then be done by using the device's arrow and enter keys, and following menu-driven instruction or voice instruction over the cellular phone. Only the replacement phone number needs to be entered as the old number is called up and deleted automatically.

In yet another embodiment, the inventive anti-theft/anti-intrusion warning and control system can be applied to protected areas, such as agricultural fields, remote villages surrounded by perimeter fences, military or defense installations, or outdoor industrial and manufacturing facilities. The sensors used in this system for detection of an illegal entry into a protected area include light beam detectors, infra-red detectors, metal detectors, etc. Optionally, a video camera with a processor, modem, and monitor can be provided to facilitate remote surveillance.

As explained above, the sensors detect an illegal entry, and the system operates to establish communication with, for example, the owner of the protected property or area, or with any of the authorized receivers of warning notices provided by the warning and control system from stored lists of pre-programmed telephone numbers. Communication is by a telephone call placed over wireless, cellular communications, to a cellular telephone, a wired telephone line, a PC, or any similar telecommunication device. Upon answering the call, the notified party receives an audio message, either by voice or by a warning tone, that there is an illegal entry. The exact location of the illegal entry into the protected area can be determined by the warning and control system using sensor technology as is known to those skilled in the art.

In still a further alternative embodiment, the inventive warning and control system can be applied to protecting valuable home appliances and movable equipment, such as a television, computer installation, and machinery such as a farm tractor. Using motion sensors installed in a hidden location on the equipment, detection of unauthorized movement of the equipment is possible, so that when such movement is detected, the system operates to establish communication with the system subscriber, or alternate pre-selected telephone numbers, by a telephone call placed over wireless, cellular communications, to a cellular telephone or wired telephone line. Upon answering the call, the authorized receiver of warning notices receives an audio message, either by voice or by a warning tone, that there is an illegal motion.
Other features and advantages of the invention will become apparent from the following drawings and description.

**BRIEF DESCRIPTION OF THE DRAWINGS**

For a better understanding of the invention with regard to the embodiments thereof, reference is made to the accompanying drawings, in which like numerals designate corresponding elements or sections throughout, and in which:

Fig. 1 is a block diagram of a preferred embodiment of an anti-theft warning and control system for a vehicle, constructed and operated in accordance with the principles of the present invention; and

Fig. 2 is a flowchart diagram illustrating the operation of the system of Fig. 1.

**DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS**

Referring now to Fig. 1, there is shown a block diagram of a preferred embodiment of an anti-theft/anti-intrusion warning and control system 10 for vehicles, constructed and operated in accordance with the principles of the present invention. System 10 comprises a sensor input unit 11, cellular transceiver 12, typically a cellular telephone capable of wireless communication via a telephone network 14, a dual tone multi-frequency detector (DTMF) unit 16, a code detector unit 18, and a local user interface, such as keypad 20. Alternatively, a bio-sensor device 22 is provided for more rapid communication with system 10. Other components of system 10 comprise an alarm unit 24 connected to an alarm device 26, a sensor detector unit 28, an auto-dialer/tone generator unit 30 with an internal memory storage unit 32, and an output unit 32. Optionally, inventive system 10 is provided with an emergency alarm switch 33 for rapid, local activation of system 10.

In one embodiment of the invention, the warning and control system 10 is powered via connector 34 by a 12v power supply 36, and has a battery backup unit 38, such as is provided by a standard 9v battery. System 10 communicates through a telecommunications network 14 with at least one remote telephone, such as at least one of telephones 40 and 42, via either a conventional wired telephone connection (POTS) 44, or via a cellular service provider (CSP) 46 for wireless cellular communications. Other modem-enabled communication devices, such as a PC 48, can also be used.
Each of the units comprising system 10 is now described, in an application relating to a vehicle protected by warning and control system 10. In this application, the warning and control system user is the vehicle owner.

DTMF detector unit 16 is coupled to transceiver 12 such that tones transmitted over transceiver 12 from one of remote telephones 40, 42 can be detected by DTMF detector 16, with each detected tone representing a code which can be read by code detector/processor unit 18. Typically these tones are generated by keying in a sequence of numbers on a telephone keypad of the remote telephone. Alternatively, any modem-enabled communications device, such as PC 48 can also be used to communicate with warning and control system 10.

Code detector unit 18 may also receive codes from local keyboard 20 in warning and control system 10, from biosensor unit 22 which, in one embodiment, is a fingerprint reader, from a voice recognition system (not shown), or from other biosensor devices as is known to those skilled in the art. Alarm unit 24 receives the codes detected by code detector unit 18, as well as a trigger signal 50 provided by sensor detector unit 28. The trigger signal 50 is provided in response to a condition associated with an entry into a warning and control system-protected vehicle, such as by opening a door, window, trunk or engine hood. The sensor detector unit 28 typically is connected to one or more sensor switches mounted in each of these areas, to establish the vehicle condition. Examples of sensor switches are indicated in Fig. 1 grouped as a class of Inputs 52.

Sensor detector unit 28 also provides auto-dialer/tone generator unit 30 with a signal 54 causing transceiver 12 to dial a telephone number, which has been pre-selected and stored in its memory 32. The sequence of pre-selected telephone numbers can be established in accordance with the user’s preference, such that the user’s telephone is dialed first, and after that, a second and third telephone number can be dialed as back-up, to insure communication with one of these telephones.

In operation, when sensor detector unit 28 detects a condition associated with an entry into a vehicle, it provides signals 50 and 54, and transceiver 12 automatically dials a telephone number stored in the memory 32 of auto-dialer unit 30. The party receiving this telephone call, who may also be the vehicle owner, is alerted to the vehicle entry, typically via an audio tone generated by a tone generator, a component of unit 30, and the alerted party is given a certain time period in which to act. At the same time, alarm unit 24 is activated, and system 10 begins to perform the sequence of steps outlined in the flowchart of Fig. 2. These steps include waiting a predetermined time interval for a secret code to be detected by code detector 18, which may be provided by the alerted party by keying in a sequence of numbers on telephone keypad 20 for identification, or, alternatively, providing a finger or thumbprint utilizing a bio-sensor 22 if the vehicle entry is authorized, and not illegal. By dialing the secret code, the alerted party stops system 10 operation.
The biosensor 22 can be programmed to read several different authorized prints for multiple users of the vehicle and has the added advantage of being much faster to activate than keying in a code in a keypad.

If the vehicle entry is made by the vehicle owner, so that it is a legal entry, the vehicle owner may dial the secret code into local keyboard 20 provided in system 10, to stop its operation.

If the vehicle entry is illegal, it is assumed that theft of the vehicle may be in progress, and in this situation, the alerted party is interested in having remote control of various functions in the vehicle, in an attempt to thwart the vehicle theft. Thus, the alerted party receiver does not dial the secret code in response to the alerting call, so that the already activated alarm unit 24 proceeds to provide a signal 56 to output unit 32, which contains relay contacts, and various devices on the vehicle. (grouped as Outputs 58) are then automatically operated. These devices allow the alerted party to instruct the system 10 to cause an interruption in fuel flow to the vehicle engine, by shutting a fuel valve 60, or to signify a theft in progress, by illumination of the blinker lights 62, if desired, in a pre-determined on-off flashing pattern. Other possible remote control functions include activating electric door locks, or setting off the vehicle alarm siren, to draw attention to the stolen vehicle. Other functions may also be provided as indicated in Outputs 58.

The warning and control system 10 also provides for a video or audio monitor unit 64 connected to sensor detector unit 28 for remote monitoring via cellular transceiver 12. A remote video/audio system 66 provides for real-time monitoring of devices, systems, and components of a vehicle or recording of such data. A remote user can also dial into the system 10 and operate the monitoring unit 64 through the output unit 32 since the monitoring unit 64 is simply another device controllable by remote code operations.

The system 10 may be implemented in a microprocessor, as known to those skilled in the art of electronic design techniques.

Referring now to Fig. 2, there is shown a flowchart diagram illustrating the operation of the system 10 in the vehicle protection application, in response to an entry into the vehicle.

The operation begins in start block 70, with initialization of the system 10 status. In block 72, if the system 10 detects a condition associated with an entry into the vehicle, such as a vehicle door being opened, system 10 operates in block 74 to dial the pre-selected telephone number via auto-dialer unit 30 to alert the system user. In block 76, a thirty second waiting interval is initiated, during which system 10 waits for entry of the secret code by the system user, or alerted party.

In block 76, one of three alternatives may occur, depending on whether a code is entered or not. If the secret code is entered by the alerted party from a source external to the system 10, such as over the telephone connection from the remote telephones 40, 42, the dialing sequence stops in
block 78, since communication has been established. If the secret code is entered by the vehicle owner on local keyboard 20, the dialing sequence stops in block 80.

If no code is entered in block 76, the waiting period ends in block 82, and in block 84, a second pre-selected telephone number is dialed by automatic dialer 30. In block 86, one of three alternatives may occur, depending on whether a code is entered or not, as before. If the secret code is entered by the alerted party from a source external to the system 10, the dialing sequence stops in block 88. If the secret code is entered by the vehicle owner on local keyboard 20, the dialing sequence stops in block 90.

If no code is entered in block 86, the waiting period ends in block 92, and in block 94, a third pre-selected telephone number is dialed by automatic dialer 30. In block 96, one of three alternatives may occur, depending on whether a code is entered or not, as before. If the secret code is entered by the alerted party from a source external to the system 10, the dialing sequence stops in block 98. If the secret code is entered by the vehicle owner on local keyboard 20, the dialing sequence stops in block 100.

If no code is entered in block 96, then in block 102, the alarm unit 24 proceeds to provide a signal 56 to output unit 32. After a five minute delay initiated in block 104, various devices on the vehicle are then automatically operated in block 106. By entry of pre-selected and programmed additional codes, individual devices connected to output unit 32 may be operated. An emergency signal is activated in block 108 through relay contacts in output unit 32, and operation of the system returns to block 74. The dialing sequence is repeated in case the initial dialing attempts were all unsuccessful, perhaps because there is no cellular telephone reception in the vehicle location area.

Alternative embodiments of the inventive anti-theft/anti-intrusion warning and control system include an embodiment applicable to enclosed environments, such as homes, offices, and commercial premises, to operate a hidden, remote control camera, which can be connected to a hidden video recorder, to record the illegal activity. The system can also provide controlled operation of accessories such as an air conditioner, or other electrical devices, such as lights.

Another alternative embodiment of the inventive system can be applied to open areas to be protected, such as agricultural fields, remote villages surrounded by perimeter fences, military or defense installations, and outdoor industrial and manufacturing facilities.

A further alternative embodiment of the inventive system can be applied to valuable home appliances and movable equipment.

Thus, the inventive system advantageously uses wireless, cellular communications to enable a vehicle owner, or home/business owner to be notified of a theft in progress or intrusion, and to
enable remote control of devices or functions designed to thwart the attempted theft or intrusion, and optionally to record the illegal activity using hidden audio or video devices.

Having described the invention with regard to certain specific embodiments thereof, it is to be understood that the description is not meant as a limitation, since further modifications may now suggest themselves to those skilled in the art, and it is intended to cover such modifications as fall within the scope of the appended claims.
We claim:

1. An anti-theft/anti-intrusion warning and control system comprising:
   a sensor input unit for reporting information about the status of at least one of a sensor-
   protected vehicle, property and area;
   a sensor detector unit for monitoring and reporting information received from said sensor
   input unit;
   a cellular transceiver for communicating over a telecommunications network;
   an auto-dialer/tone generator unit for dialing at least one pre-programmed telephone number
   and generating a warning tone via said transceiver in response to detection of a
   security threat;
   a memory unit connected to said auto-dialer for storing at least one pre-programmed
   phone number for said auto-dialer unit to access and dial;
   at least one user interface for inputting at least one secret user code to access said warning
   and control system;
   a dual-tone, multi-frequency (DTMF) detector unit for decoding tones received by
   said transceiver into said at least one user code;
   a code detector/processor unit for comparing said at least one user code with at least one
   pre-programmed code stored in said warning and control system;
   an alarm unit for activating at least one alarm and arming at least one anti-theft/anti-
   intrusion security measure associated with said at least one of protected vehicle,
   protected property and protected area in accordance with the code detector/processor
   unit comparison of said at least one user code and said at least one pre-programmed
   code; and
   an output unit for executing said at least one anti-theft/anti-intrusion security measure.

2. The anti-theft/anti-intrusion warning and control system of claim 1 further comprising:
   a battery back-up unit to provide emergency electrical service to said warning and
   control system independently of any existing electrical service associated
   with said at least one of protected property and protected area;
   an emergency alarm switch for communicating an alarm signal directly to said
   at least one authorized receiver, while simultaneously activating pre-
   programmed said at least one anti-theft/anti-intrusion security measure; and
a monitoring unit for monitoring signs of said security threat to said at least one of
guarded property and protected area.

3. The warning and control system of claim 2 wherein said monitoring unit comprises at least
one videocam and a broadband transmission system for real-time broadcast of images from
surveillance of at least one of said protected property and protected area to a
remote station for monitoring.

4. The warning and control system of claim 2 wherein said monitoring unit comprises at least
one audio system for broadcast transmission over said telecommunication network to a remote
station for monitoring.

5. The warning and control system of claim 1 wherein said warning is effectuated by passive
sensory alarms.

6. The warning and control system of claim 1 wherein said control function comprises
disabling, enabling, activating or deactivating at least one of a device, portion of a device,
component, system, sub-system, and/or function associated with at least one of a protected vehicle,
aprotected property, and a protected area.

7. The warning and control system of claim 6 wherein said protected vehicle comprises a
conveyance selected from the group: an automobile, a truck, a semi-trailer, a tractor-trailer, a
railroad train, a bus, a forklift, a golf cart, a snowmobile, a motorcycle, a motorbike, a recreational
vehicle, a mobile home, a trailer, a marine vessel, a ship, a boat, an aircraft, a jet aircraft, a lighter-
than-air ship, a dirigible, a blimp, a zeppelin, a space satellite, a space ship, and agricultural and
construction conveyances.

8. The warning and control system of claim 6 wherein said protected area comprises a
designated area whose perimeter is marked by at least one of a fence, border markings, natural
geographical features of the terrain, and the like, so as to be guardable.

9. The warning and control system of claim 6 wherein said at least one of a device, portion of
a device, component, system, sub-system, and/or function of said protected vehicle comprises at
least one of electrical, mechanical, aeronautical, navigational, hydraulic, and electromagnetic
systems and subsystems, and further comprises at least one of a vehicle fuel system, ignition system, lighting system, and locking systems for doors, windows, engine compartment, emergency exits, and storage compartment.

10. The warning and control system of claim 1 wherein said information comprises at least one of a use; attempted use, and theft of at least one of a protected vehicle.

11. The warning and control system of claim 1 wherein said transceiver communicates with at least one of a digital phone, a cordless phone, a wired telephone, a cellular phone, a computer, a PC, a modem-enable TV, a beeper, and a PDA (Personal Digital Assistant).

12. The warning and control system of claim 1 wherein said emergency alarm switch is programmable to communicate at least one of an alarm signal and a recognizable tone directly to said at least one authorized receiver via said cellular communications device and also to activate said at least one security measure.

13. The warning and control system of claim 1 wherein said at least one security measure is provided by an array of more than one warning and control system, each operating independently of one another.

14. The warning and control system of claim 13 wherein said array of more than one warning and control system is provided to said at least one of a protected vehicle, a protected property, and a protected area when said at least one of a protected vehicle, a protected property, and a protected area are too large for a single said warning and control system.

15. A warning and control method comprising the steps of:
   initializing the warning and control system status;
   monitoring at least one of a vehicle, a protected property, and a protected area; accessing said warning and control system;
   detecting a security threat to at least one of said vehicle, protected property, and protected area;
   activating an alarm to alert others to said security threat;
   establishing at least one communications link over a telecommunication network to at least one authorized receiver of said security threat notice;
sending a first secret code response back to said warning and control system from
said at least one authorized receiver;
utilizing said first secret code to activate at least one security measure provided by
said warning and control system to thwart said security threat; and
sending a second secret code to said warning and control system to return the
warning and control system to Standby mode after said security threat has
been counteracted; and
communicating additional secret codes to said warning and control system to
monitor and operate selected devices, functions, and systems affecting the
general operation and security of said at least one of said protected vehicle,
protected property, and protected area.

16. The warning and control method of claim 15 wherein said initializing, accessing,
monitoring, and activating functions are remotely performable utilizing secret codes transmitted
over a telecommunication network.

17. The warning and control method of claim 15 wherein said monitoring comprises video
and/or audio surveillance.

18. The warning and control method of claim 15 wherein said secret codes are remotely
programmable.