REVIEW OF PRESENT STATE OF THE ART OF RESIDENTIAL FIRE AND BURGLAR ALARM HARDWARE

Tom D. Smith
Director of Operations
Communications Products Group
Scientific-Atlanta, Inc.
Atlanta, Georgia

ABSTRACT

The present residential alarm hardware and system configuration is described for cable management and technical personnel who are interested in providing this ancillary service over a two-way cable system. The advantages and disadvantages of wired and wireless systems, perimeter and volumetric intrusion sensors, as well as heat and smoke protection, are described. Important features of the alarm control panel and various methods of communicating to the central security station are discussed. Pictures of current hardware are included. The conclusion identifies unique advantages of a cable television company offering alarm services.

BACKGROUND ON THE ALARM MARKET

For many cable industry people, the recent interest in monitoring fire and burglar alarms over cable communication systems is a return to the late 60's and early 70's when several manufacturers offered interactive cable terminals. It is interesting to note that Scientific-Atlanta designed and demonstrated interactive two-way cable terminals in 1969 to monitor residential fire and burglar alarms before it developed a line of distribution equipment.[1] (See Figure 1.)

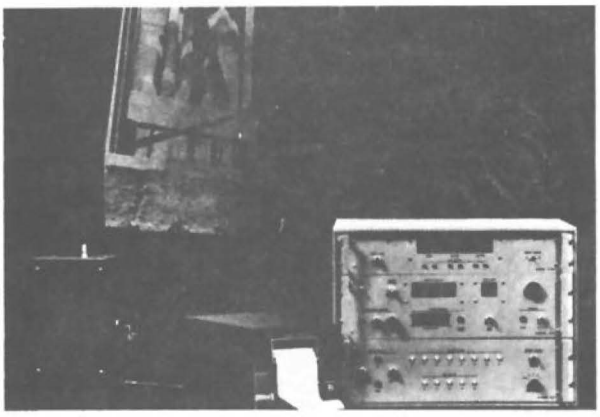


FIGURE 1. 1969 Alarm monitoring system for cable television

Although the two-way cable market didn't develop in the 70's, this early involvement with residential alarm systems resulted in a major contract for Scientific-Atlanta to supply residential fire and burglar alarm systems to Rollins Protective Services Company in 1971. Through this arrangement Scientific-Atlanta has become a leading supplier of residential alarm systems, having well over 40,000 installed systems.

Until recently most alarm service companies have concentrated in the commercial and industrial market. The residential market has presented unique and expensive marketing problems. Fewer than 2% of U.S. homes are now outfitted with security systems. Thus, the potential market includes almost all the nation's 75,000,000 existing residences. Creative Strategies, a marketing research firm in San Jose, California, estimates that installed sales will total $395,000,000 by 1985. Gallup Polls estimates that one in every four houses was hit by crime within the last year, and that 20% of the U.S. population doesn't feel safe, even at home. The time seems right for an effective, affordable protection system.

The cable communications system and the cable door-to-door marketing offers a unique opportunity to provide a needed service to the consumer and a profitable ancillary service to the cable industry.

A security system consists of three major elements: sensors, a control unit, and an alarm. The sensors detect an intrusion or fire. The fire sensor is usually a smoke detector, that is a device which detects the presence of smoke or other products of combustion. The intrusion sensor, however, can take many forms. The most commonly used is a special switch that opens when windows and doors are opened or broken into. The control unit turns the system on or off and monitors the sensors. When a sensor is tripped, that is, a set of contacts is either opened or closed in the sensors, the control unit will sound the alarm, which is normally a siren or bell. Most control units also contain an automatic communicator which signals over telephone lines or a cable television system to a central monitoring station. This signal identifies the customer, the location, and the nature of the emergency. The answering service then notifies the proper authorities. A block diagram of the system is shown in Figure 2.

Alarm systems can be further subdivided into wired systems, where all sensors are wired to the control unit, or wireless systems, where the sensors are connected to the control unit via radio or some other nonwired communication channel. Most

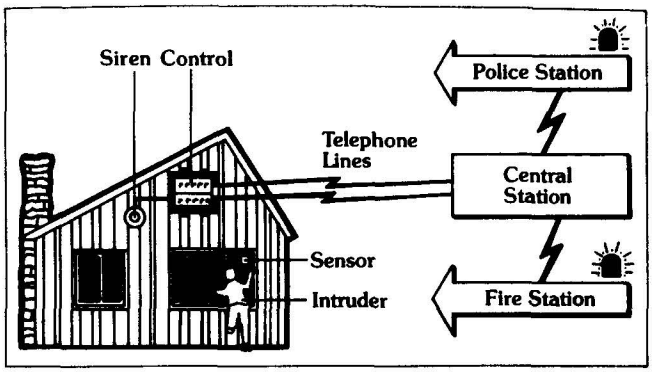


FIGURE 2. Block diagram of security system answering service

wireless systems use a radio link between the sensors and the control unit. The sensor's transmitter frequency, power output and transmission duration are controlled by the Federal Communications Commission Regulation Part 15. Compliance to these Rules constrains the equipment designer in providing an effective alarm system. The FCC has proposed new Rules (Docket 20990, dated November 1, 1976) which may improve the equipment design options. But until these new Rules become effective, the radio equipment must comply with the present Rules and be certified by the FCC. The advantages and disadvantages of a hardwired and a wireless system are outlined in Figures 3A and 3B.

Advantages of a Wired System

1. Sensors are supervised, systems cannot be turned on with doors and windows open
2. System hardware cost is less than a wireless system
3. Sensor powered from master control unit
4. Zoning is possible
5. Equipment doesn't require FCC approval and neighboring system cannot interfere

Disadvantages of a Wired System

1. Requires considerable on-site labor running wire from control unit to sensors
2. Exposed wires are often objected to by homeowner
3. Installed cost is usually more than a wireless system

FIGURE 3A

Advantages of a Wireless System

1. Requires less on-site labor running wires
2. Installation less conspicuous
3. Portable or hand-held sensors possible
4. Easy installation for homes already constructed

Disadvantages of a Wireless System

1. Range of transmitter limited
2. Batteries must be replaced periodically
3. Zoning is usually not possible
4. Equipment must comply with FCC Rules Part 15
5. Supervision of sensors not possible
6. System can be turned on without detecting open doors and windows
7. Subject to interference from neighboring systems

FIGURE 3B

INTRUSION PROTECTION

Intrusion protection sensors are divided into a perimeter sensor and a space or volumetric sensor. A perimeter sensor detects an intrusion through the perimeter of a building or area, such as the opening of a door, a window, or gate. The volumetric sensor protects a defined volume and senses whenever there is an intruder in this volume.

The most popular perimeter sensor is a magnetic switch. (See Figure 4.) This sensor consists of a permanent magnet and a magnetically activated switch. When the switch is in close proximity to the permanent magnet, the switch is closed. When the two units are separated, the switch opens, indicating an intrusion. This type of sensor is usually installed on doors and movable windows.

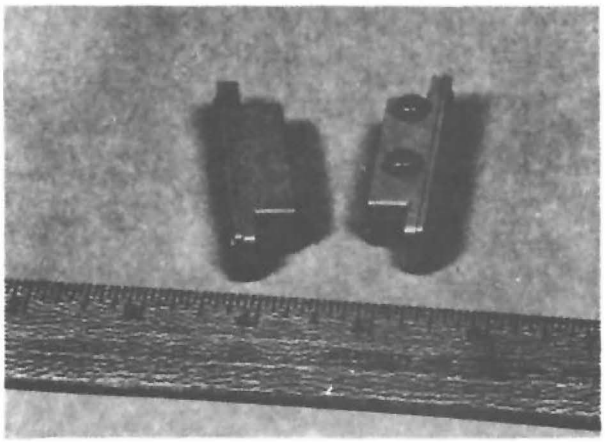


FIGURE 4. Magnetic switch

Pressure type switches can also be used to detect window and door openings, by arranging the switch so that when the window or door moves the circuit is open. (See Figure 5.)

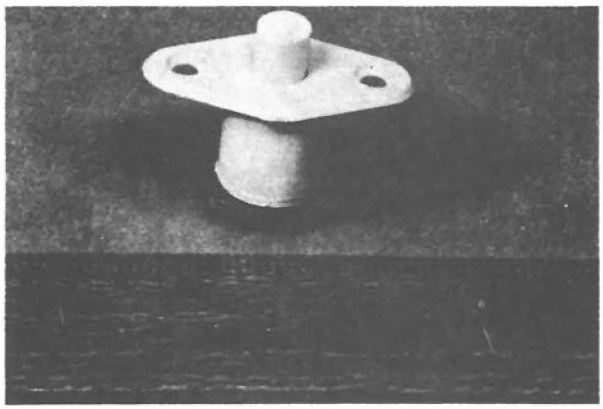


FIGURE 5. Pressure switch for windows and doors

Large plate glass windows can be protected by a thin foil circuit taped to the perimeter of the window. This foil circuit will open should the window be broken. Another technique for protecting large plate glass windows is the so-called glass break detector. This unit consists of a

small transducer mounted on the glass window. (See Figure 6.)

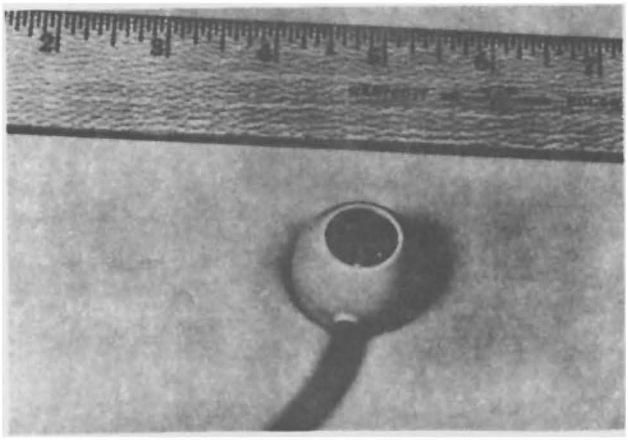
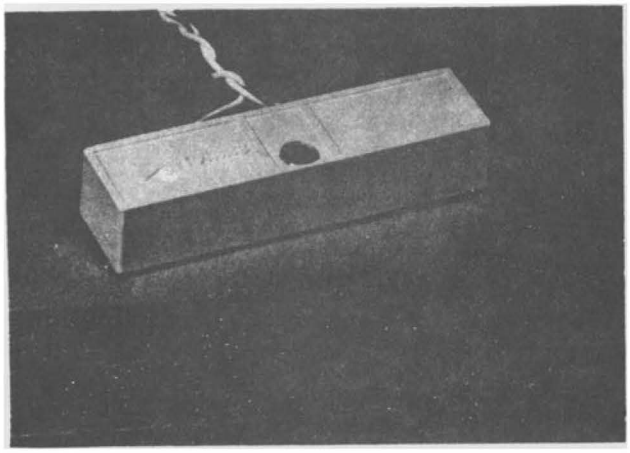


FIGURE 6. Glass break detector

This transducer is tuned to the frequency of breaking glass and opens a switch when the glass breaks. This has the advantage of minimizing the labor involved in taping the perimeter of large plate glass areas. Another type of window protection is a vibration detector. (See Figure 7.) This device consists of a weighted switch, which momentarily opens with the shock of breaking glass. This device can also be used to detect vibrations caused by penetration of walls.



FIBURE 7. Vibration Detector

Another type of perimeter detector is the photoelectric eye. The photoelectric eye consists of an optical or infrared light source and a receiver. The transmitter and receiver are placed so that an intruder entering a perimeter will break the light beam. When the light beam is broken, an alarm is sounded. The light source is usually pulsed in a coded manner in order to avoid jamming by external light sources.

Initial perimeter protection can be backed up by additional perimeter protection, such as mat switches, which are placed under rugs or carpets to detect intruders. The basic security systems are often backed up with panic buttons or manually activated switches to start an alarm sequence.

A volumetric sensor, as the name implies, is designed to detect the presence of an intruder in a specified volume of space. The most popular form of volumetric sensors is the ultrasonic motion detector. This motion detector works similar to a police radar. An alarm is sounded any time the sensor detects motion in the area covered by the detector. A microwave motion detector works on the same principle as the ultrasonic detector, except microwave frequencies are used to detect motion rather than ultrasonic sound waves. The microwave motion detectors are somewhat more expensive than the ultrasonic detectors and they also provide better control of the space to be protected. Another volumetric sensor that is gaining acceptance is the passive infrared detector. This device senses the heat radiated by an intruder. Balancing circuitry inside the infrared heat detector keeps it from being sensitive to ambient temperature changes and constant light sources.

Volumetric sensors tend to find their application in protecting areas in which the occupancy can readily be predicted, such as commercial and industrial buildings. The problem with volumetric sensors in homes is that any movement by the homeowner or house pets, even air movement caused by the heating and air conditioning fan, can sometimes cause an alarm.

FIRE DETECTORS

Thermal detectors, or heat sensors (See Figure 8) are activated when the detector element exceeds a predetermined temperature. While heat detectors are useful in minimizing the damage to a protected residence, they may not offer much life protection.

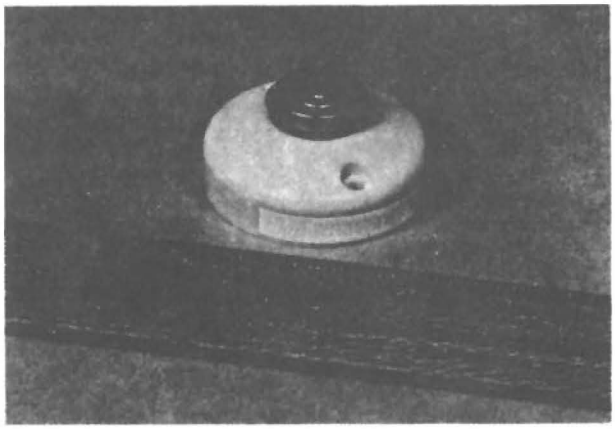


FIGURE 8. Thermal detector

Most fire casualties are caused by smoke inhalation, as opposed to heat. Unless the thermal detector happens to be in close proximity to the origin of the fire, it is not likely to detect the fire in time to ensure the safety of the occupants. Therefore, most residences are now being outfitted with smoke detectors. These smoke detectors can give a much earlier warning of conditions that are likely to be unsafe for humans. Smoke detectors work either on a photoelectric principle or an ionization principle, or a combination of the two.

Photoelectric smoke detectors operate on a light principle, reacting when smoke obscures the beams path or reflects light into the photocell located inside the detector. With an ionization detector, the air within a small chamber is electrically conducted (ionized) by the emission of alpha rays. Combustion particles entering the chamber cause a change in the current flow, which results in an alarm. Some smoke detectors use a combination of both principles to improve the detection of all types of fires. A typical smoke detector is shown in Figure 9.

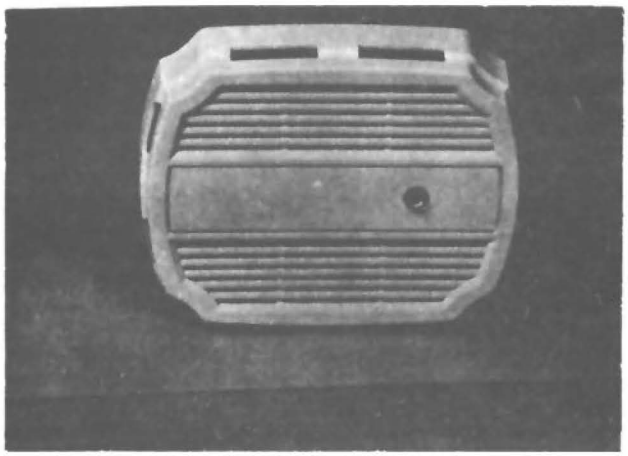


FIGURE 9. Smoke detector

CONTROL SYSTEM

The control unit is the heart of the alarm system. (See Figure 10.) It allows the customer to select the security mode or level. It also provides housing for the alarm processing electronics, batteries for emergency power, and the communication device to relay the alarm to the central station. If the system is a wired system, the wires from the sensors located throughout the protected premises are brought to the control unit. If the system is a wireless system, the control panel generally will also house the radio receiver which receives the messages transmitted by the wireless sensors.

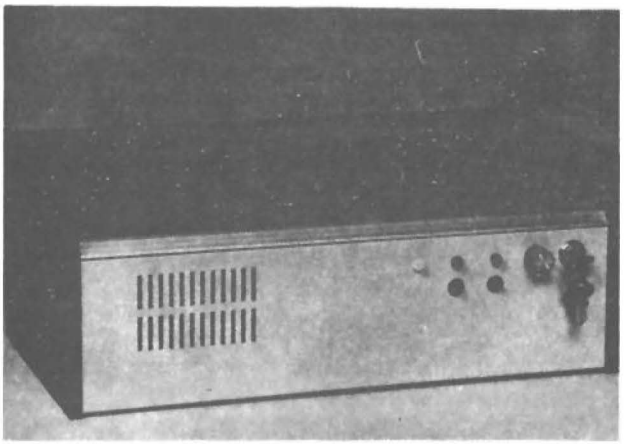


FIGURE 10. Control unit

The customer can turn on the intrusion alarm either with a key with is removable, or a keyboard entry which consists of a customer secret code followed by a command to indicate system on or off. The fire alarm is usually on regardless of whether the intrusion alarm is on or off. Some sophisticated control panels have a zoning feature, i.e., a portion of the system can be on while another portion of the system can be turned off. For example, if people are at home and confined to the main living space, that portion of the system can be turned off. The normal going and coming through the main living space would not set off the alarm, while the intrusion alarm in the basement and the upstairs can be left on to detect any would-be intruder. Most alarm control units have an entrance and an exit delay built into the system. This delay allows the homeowner to turn the system "on" and leave the house without setting off the alarm. Conversely, the entrance delay allows the owner to enter the house and turn the system "off" before the alarm goes off. The control unit allows these delays to be adjusted from 10 seconds to 45 seconds. U.L. Specification No. 1023 specifies that the maximum delay shall not exceed 45 seconds. Most alarm controls sound a low volume beat, while in the entrance delay mode, indicating that within a short period of time the alarm will sound if the system is not turned off. This warning also helps to reduce false alarms caused by accidental setting off of the alarm.

Sometimes entrance and exit delays are not convenient. In this case, a shunt lock can be wired in series with a sensor, which will allow the homeowner to open a specified door to enter and exit the home without setting off the alarm. The shunt lock is usually mounted outside the door that is commonly used to enter and exit the home without setting off the alarm.

Most residential alarm systems will provide for a loud local alarm, such as an electronic siren or an outside bell. This local alarm serves several purposes: (1) it alerts the neighbors that an intrusion or fire has taken place; (2) it alerts the occupants of a fire or intrusion; and (3) in the case of an intrusion, hopefully it will frighten the would-be intruder away. The control unit must provide two distinct alarms: one sound for intrusion, the other sound for fire. U.L. 1023 requires that minimum sound levels should be 85 dB at 10 feet. A reset timing circuit is desirable so that at the end of a 4-10 minute alarm the system automatically resets, thus eliminating the necessity of someone entering the home to turn the alarm off. U.L. 1023 requires a minimum of four hour emergency stand-by power. This is normally supplied by one or more batteries which are continuously being charged while primary power is available.

COMMUNICATION TO THE CENTRAL STATION

Many alarm systems depend on the local alarm only. The local alarm theory is that the would-be intruder would be frightened away and neighbors or

passers-by, on hearing the alarm, would report the alarm. The next step up in system sophistication is the automatic telephone dialer. This communication device is usually located inside the control unit, and when the outside alarm sounds, it seizes the telephone line and dials the central station and reports either an intrusion or a fire message. The central station then sends the appropriate authorities to the identified residence.

Many early automatic telephone dialers dialed the police department directly, but because of the number of false alarms received and because some of the telephone dialers had a tendency to jam the switchboard at the police or fire station, most city authorities enacted ordinances which forbade dialers from directly phoning the emergency and fire numbers. Most alarm service companies therefore provide a central station to intercept these messages. They in turn follow the emergency procedures that the customer has provided. The central station not only will call the appropriate authorities, but many times will notify neighbors and friends, and will call the owner at work if the emergency occurs during working hours.

One of the main deficiencies of the automatic telephone dialer is the possibility of a would-be intruder cutting the telephone wires prior to break-in. This will revert the system to local alarm only. The cutting of the telephone lines with an automatic telephone dialer cannot be detected at the central station. In order to overcome this difficulty, dedicated telephone lines can be provided from the protected residence to the central answering station. This type of protection has been quite popular with commercial and industrial installations but is expensive for homeowners. Also, the availability of these circuits has become very scarce. The telephone company with its multiplexing system can get twenty or more voice channels out of a single copper pair, but if the copper pair is used to provide security protection to the central answering service, it can serve only one customer. Therefore, the telephone company has little economic incentive to provide these circuits.

Interactive two-way cable systems revolutionize the economics in remotely monitoring residential fire and burglar alarms. A central computer can periodically interrogate the security terminal located in customers' homes, and determine if the system is working and if there is an alarm. Because of the broadband "party line" nature of the cable system, interrogation can be done rapidly. The telephone system cannot approach this performance, because its system requires switching from one customer to the next before interrogation can begin. The cable system can tell when a line is cut, because a lack of response from a terminal is treated as an alarm. If a would-be intruder cut the cable drop before attempting to enter a protected home, it would be communicated immediately to the central station. Should a sector of the cable system go out, this interrogation process would also automatically identify and pinpoint for the cable operator where to dispatch a repair crew, without having to wait for phone calls from complaining customers.

Obviously, the approach can easily be extended to increase customer service and system reliability by incorporating a cable performance monitoring alarm into the interrogation system. These monitors could detect signal level out of specifications as well as outages.

UNIQUE ADVANTAGES OFFERED BY ALARM SERVICES OVER CABLE TELEVISION SYSTEMS

Cable operators possess several unique advantages in providing residential alarm services. The cable companies' high integrity and visibility in the community provide a unique marketing advantage. The residential security market has been plagued by fly-by-night, unethical companies. There are presently more than 15,000 local and regional fire alarm companies who install and maintain systems. An estimated 35% to 40% of these companies go out of business each year, according to a recent study by a New York based market research group, Frost and Sullivan.

Small local suppliers have neither the resources nor the interest to attack the residential market. No national company with a recognized brand name has emerged in the residential market. Cable companies already have the expertise that will be demanded to penetrate this market. The same in-the-home sales effort, the same marketing savvy, the same expertise in operating local offices, and the substantial capital to cover the front end expenses used to make the cable entertainment services successful will be necessary to make the residential alarm service successful. Few traditional alarm service companies could match these resources.

Until recently, the homeowner had two basic choices in residential alarm systems: a $2000-3000 stripped down version of a commercial system installed and maintained through a central station alarm business or various gimmicks that were low cost, self-installed and largely ineffective. Cable companies can provide the homeowner with a variety of security systems at affordable prices.

Given the unpleasant connotation of residential fire and burglaries, the home security system will require a hard, in-the-home sell strategy, like life insurance and cemetery lots. Only a very small percentage of the consumers can be convinced to voluntarily seek out and buy such products. Marketing is the name of the game in the residential alarm business, and marketing is where the cable companies have the edge.

NOTES:

[1]Marvin Roth, "Security Alert, a Two-way Digital Communications System," The 20th Annual NCTA Convention Official Transcript, National Cable Television Association, 1971.