

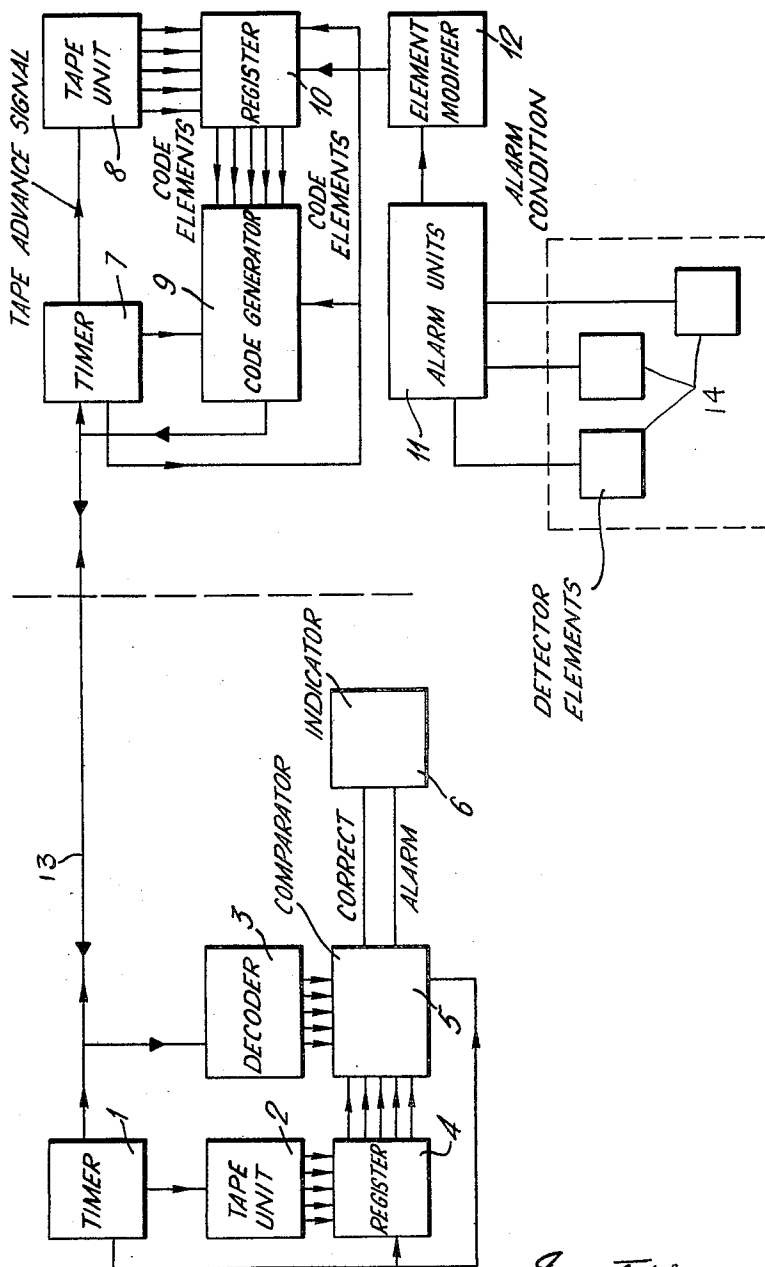
Feb. 23, 1965

J. C. MacKEEN

3,171,108

VALUABLE PROTECTION SYSTEM

Filed Nov. 23, 1960



Inventor:
John C. MacKeen
By Hemon, Palmer & Stewart
Attorneys

1

3,171,108
VALUABLE PROTECTION SYSTEM
 John Crerar MacKeen, 170 Hollis St.,
 Halifax, Nova Scotia, Canada
 Filed Nov. 23, 1960, Ser. No. 71,311
 10 Claims. (Cl. 340-226)

2

The present invention relates to a system for indicating at a remote location an alarm condition within an area. This system is particularly useful for protecting a strong room or other location containing valuables.

The integrity of a strong room is maintained by two features: Firstly, the construction is such as to delay entry by improper means, and secondly, the room is watched or supervised at intervals which are less than the access times. The implementation of both these features is limited. Both of these features have inherent limitations. The delay imposed on an improper entry is limited by construction costs and is in any event, inversely dependent upon the scale of the effort available to force entry. The supervision over nonworking periods, is generally by a very limited force, who may be overpowered or forced into cooperation. It also frequently occurs that the access route is not supervised, for example, when a wall or floor is penetrated from another building. The essentials of an efficient protection system are these: Firstly, that the supervision shall be from the interior of the room, and shall be continuous, and secondly, the supervision shall communicate with a central location where a sufficient number of people can be located to deal promptly with an attempted entry. Economics dictate that these people shall either have other duties or responsibility for many installations, e.g. Protection Company. Thirdly, its link between the room and the central location must be completely secure.

The supervision facilities at the room utilize current state of the art devices. They will be arranged to provide a common type of indication of an alarm condition. Any combination of facilities will thus be available for connection into the alarm registering unit of the special equipment later described.

The facilities available are:

Systems registering conditions outside the room walls, which would indicate an attempted entry.

(a) *Sound or acceleration pickups.*—Small microphones or acceleration transducers mounted on walls or framework of the room to register an increase in ambient noise or shocks resulting from blasting, hammering, drilling, chiselling or supersonic cutting.

(b) *Thermal pickups.*—Thermal units which may be mounted directly on walls or built into the protective masonry to indicate local rise in temperature, or may be located within the room within a reflector type array to view larger wall areas.

These units will indicate any rise in temperature resulting from burning or attempted flame cutting.

(c) *Strip or continuous conductor.*—A continuous wire or strip worked into the fabric and onto inside walls to be broken by attempted penetration of masonry or by penetration of the wall. This system would also cover doors and other potential points of entry.

A second type of facility indicates movement past a barrier or within an area. In certain conditions, the devices of the previous group might not provide protection, for example, in a large room a person might remain concealed when the room was closed, operate during the closed period, and leave the area during the open period. Or, the area to be protected might not be a strong room in itself, but perhaps only a vital area within a larger open area, as for example, an unusually valuable consignment in a warehouse. Under these conditions, there

are two types of systems available. Firstly, there are systems to provide a barrier which cannot be passed without alarming.

- (a) Optical beams visible or infra red.
- (b) Supersonic beams.

These devices consist of a source and detector, and provide a fence type of protection. It can be made impossible to pass even a small object through this fence without causing an alarm. Such a system will close off a passage and by suitable choice of frequency and other parameters, can be designed to detect the "fishing" type of theft, by which articles are removed from without the area. Secondly, a whole area may be arranged so that movement of any object in it will provide an alarm. This type of system is most fitted for areas which are wholly enclosed by walls which provide an efficient barrier to the radiation employed. The area to be protected is provided with one or more detectors and a radiator. The radiator is more or less centrally disposed and emits radio or supersonic energy. This energy is received on the detectors. Any displacement within the area of reflecting or absorbing material, will alter the received level on a suitably positioned detector, and this may be arranged to cause an alarm. The above devices are available in various forms, but would require engineering into an overall system for the purpose of this paper. Such devices do not form part of the invention but may be used with apparatus in accordance with the invention to provide a security system.

In accordance with the present invention a system is provided for transmitting to a remote location an indication of an alarm condition within an area, said system comprising an interrogation device adapted to interrogate a coded responder adjacent said area, the reply by said responder to said interrogation being altered by an alarm condition. Thus, in the absence of an alarm condition a series of interrogations and responses are transmitted back and forth between the interrogator and responder which indicate that there is no alarm condition. Further, these interrogations and responses indicate the integrity of the connection link and the equipment. When an alarm condition causes an alteration in the responses or when no response is received an alarm is generated by the interrogation device and human supervision can be sent to the area.

In one form of the system in accordance with the invention, means are included within said responder adapted to generate a first coded signal in response to an interrogation from said interrogator and to alter said response after each interrogation at least one alarm unit connected to said responder, means in said interrogator adapted to generate a second coded signal and to alter said second coded signal after each interrogation, means in said interrogator adapted to compare said first coded signal with the second coded signal and to indicate an alarm condition when said first and second signals differ, and means in said responder adapted to alter said first coded signal in response to an alarm from an alarm unit.

In a system in accordance with the present invention, the human supervision is remote from the strong room, and so it is necessary to provide a link between vault and the central position. In a metropolitan area, the most practicable link is a telephone line, which may be rented from the utility. This link is not secure and for the purpose of this paper, is considered to be entirely open. It will pass in through the exchange, but can be "tied" or permanently rented to avoid switching circuits. This type of connection is a normal utility service.

In considering the security measures for this link, it is assumed that the effort to violate it will reflect the value

of the contents of the vault, and will command all state of the art available technical resources. In general, it must be assumed that the link will be accessible at several points, both to mechanical interference and to electrical interference or wire tapping. The information the link must convey, is the state of the internal alarm devices of the vault. The system must ensure that the link is actually connected to the internal alarms at all times, and that no information is being added or removed from the link.

The nature of potential interference is as follows: in a system where a circuit is opened, e.g., wires which are broken, conducting strips on glass, contacts on doors. The intruder would bridge the wires before breaking in. In systems depending upon closing a circuit, the wires would be severed. More sophisticated systems might generate a tone which varied in an alarm condition, or a complex train of information corresponding to the states of several alarm systems, but it must be assumed that any system which transmits repetitive regular or consistent information, will be vulnerable to the following process. The outgoing information would be recorded from a wire tap. The record would be studied and the pattern of the information corresponding to a secure condition would be ascertained with more or less effort. A simulated signal corresponding to the secure condition could then be applied to the line and the internal system disconnected. Simulator technique of this kind requires only skill and effort, and will defeat any repetitive or consistent system given a sufficient "Sample."

It is proposed, therefore, to use a system transmitting purely random information. The central station will send out an interrogation signal to the vault. On receipt of this signal, the vault unit will reply with a signal containing one or more "bits" of binary information. The composition of this reply will have been set up from a single code group of one of a pair of identical masters or tapes. Upon receipt of the return, the reply will be examined automatically for identity, with the corresponding code line on the duplicate master at the central station. If the correspondence is exact, i.e., no errors or omissions, the central unit will not alarm, and will prepare to send a further interrogation signal after an interval. Upon receipt of the next interrogation, the vault unit will reply with the next code group of the sequence, which will be compared with the corresponding line by the central unit, which also advanced its master one line prior to sending out the interrogation.

Any error or omission in the reply code, will cause an alarm condition at the central unit. It is proposed that an alarm condition at the vault should change the sense of one or more elements of the transmitted code group. This transposition will result in an alarm at the central station. There will be no indication on the line of the alarm conditions to an observer not in possession of the appropriate code group. The vault and central tapes will be duplicates of a random series of code groups. In the system as described, the tapes at the vault and the central station are identical and initially are set to the corresponding code line. The system is secure if any tape is not transmitted more than once. This is not a serious limitation. A tape can conveniently hold at least 100,000 lines, which would provide 70 days supervision at one interrogation per minute. If an unauthorized copy of the tape exists, then the security is impaired in the simple system for the following reasons:

Assume that a sample of transmission of p groups has been intercepted, the probability of this sequence in any sequence of p groups is N^p , when N is the number of possibilities for each group (31 in 5 binary bit groups). If then, a third copy of the tape were available to the interceptor, the position of this group on the tape, could be established with little probability of error after 3 or 4 groups had been received in a tape of 100,000

groups. The searching of 100,000 groups is a rapid and simple operation by computer technique. The security of the tape is thus in this system paramount.

Since, however, one tape is within the vault and the duplicate within the central position where a simple safe would protect it, this risk is not serious if proper precautions are taken in tape manufacture. If the tape sequence is not available to the interceptor, the probability of simulation is small. If each group consists of n elements or bits, and each bit has two states, ON or OFF, there are $2n$ possible groups or $(2N - 1)$ if the condition "ALL OFF" is not used. The elements may be distinguished by time sequence or may be separate tones present simultaneously. A group of five (5) elements would offer 31 possibilities. In a purely random sequence, any inserted group of proper basic elements would have only a 1 in 31 possibility of being accepted by the central unit. The possibility of two random inserted groups being accepted, is 1 in 961, and these probabilities could not be improved by prolonged study of the information on the link. The intervals between interrogation would be of the order of minutes, so that an alarm condition could not remain long undetected at the central station.

In the system described, security depends essentially upon maintaining the tape sequence *secret*. If this secrecy is lost, the relatively short length of a practicable tape would permit a rapid search after only a few lines had been intercepted to establish position of the sequence on the tape after which further non-alarm replies could be simulated. It is also evident that no great improvement is possible by reducing the number of elements of each line or lengthening the tapes.

In accordance with the third form of the invention a system is provided which is not greatly dependent upon the security of the tape or source of sequence which is used in the system.

Two master tapes of random groups are produced as before, but each tape is split longitudinally into n separate tapes of binary information. The central and vault units embody a means by which each of the n tapes may initially be set to a different line. After initial setting the tapes will be advanced together by single line steps. The machine will thus generate N^n arrangements from the group of n tapes N of lines each. The selection of one of these sequences will be made by pre-setting the tapes to a combination or code of n numbers each number lying between 0 and N , thus a typical starting combination for a tape of 100,000 lines and 5 elements would be:

00006
00023
00101
00042
00178

and the same code would be set up at vault and central unit. The tape is now effectively 10^{25} lines long. A study of the labour involved in searching such a tape shows, however, that if the lines are transmitted by a simultaneous tone group, each tone serving to identify a column the tones can be relatively quickly identified with the separate tapes, so that the labour of searching in the case of the tape described above is only that equal to searching a single column tape of 1.5×10^6 lines. This is a computer operation which might be completed in minutes. This method of searching would also operate with a sequence group in monotone. If, however, the information transmitted is modified so that the identification of the transmitted elements with the individual tapes is lost, then the tape possibilities must be searched at full length that is, as a tape of 10^{25} lines. The method proposed is to sum the information on the n tapes for each line and transmit only a signal signifying ODD or EVEN sum of the n bits of that line. The task

of identifying the tape positions from the intercepted binary information is now that of locating the sequence in a series of 10^{25} lines. In order to achieve this it would be necessary to search this series for a sequence of over 250 lines. A search of this magnitude is not presently possible within the period of perhaps 96 hours, even with massive computers. The possession of a duplicate tape would thus not greatly benefit the interceptor. The security would now be based mainly upon the relatively short lived combinations set into the initial tape positions and the settings of these could be divided between several persons. The possibility of a single random inserted reply being accepted is now $\frac{1}{2}$ so that the interrogation rate must be raised to 5 times that required with the 5 element transmission to provide the same probability of alarm within an equal period. The operating sequence and the insertion of the alarm by code modifier remain unchanged.

In the drawing which illustrates an embodiment of the invention, reference numeral 1 shows a timer used for controlling the operation of the interrogator. Reference numeral 2 refers to a tape unit in which one or more tapes containing code groups in binary form is controlled from the timer 1 and in response to a signal from the timer it passes a signal to the register 4, the binary signal inserted in the register 4 is passed to the comparator 5 together with a signal from the decoder 3, the comparator compares the signal from the register 4 with the signal from the decoder 3 and produces a correct response to the interrogator or an alarm which is shown on the indicator 6.

The timer 1 at the same time that it sends a signal to the tape unit 2 transmits an interrogator signal via the line 13 to the responder equipment located adjacent the area to be protected. The responder includes and serves to operate the tape unit 8 which is identical with the tape unit 2. The tape unit 8 supplies a signal in binary form to the register 10 which in turn supplies a code to generator 9 and sends the response via the line 13 to the decoder 3. A plurality of detector elements 14 are located within the area to be protected. These detector elements may be of the types previously mentioned and serve to indicate that the security of the area being protected has been violated. The detector elements 14 send the signal to the alarm units 11 indicative of the condition. The alarm units 11 control the operation of the element modifier 12 which serves to modify the binary signal placed in the register 10 from the tape unit 8. The modified binary signal from the register will cause the generation of an incorrect code in the code generator 9 and this incorrect code will be sent via the line 13 to the decoder 3. The decoder 3 will thus place into the comparator 5 a signal differing from the signal from the register 4. An incorrect comparison will be obtained and an alarm will be given to the indicator 6.

I claim:

1. A system for indicating at a remote location the presence of an alarm condition in an area said system comprising, an interrogator adapted to interrogate a responder located adjacent said area at predetermined time intervals, means within said responder adapted to generate a first coded signal in response to an interrogation from said interrogator and to alter said response after each interrogation, at least one alarm unit positioned adjacent or in said area and connected to said responder, means in said interrogator adapted to generate a second coded signal and to alter said second coded signal after each interrogation, means in said interrogator adapted to compare said first coded signal with the second coded signal and to indicate an alarm condition when said first and second signals differ, and means in said responder adapted to alter said first coded signal in response to an alarm from an alarm unit.

2. A system according to claim 1 wherein said first and second signals are generated from information stored on first and second storage media, the storage media for each signal containing identical information.

3. A system according to claim 2 wherein said information is a series of binary numbers.

4. A system according to claim 3 wherein said first and second signals are electrical analogues of a binary numeral from said groups of storage media.

5. A system according to claim 3 wherein said first and second signals are a single binary digit.

6. A system according to claim 1 wherein each of said first and second signals is generated from coded information stored on first and second groups of storage media respectively, the coded information of said first group of storage media being identical with the coded information of said second group of storage media, the storage media of the first group being adapted to be scanned in the same order as the storage media of the second group.

7. A system according to claim 6 wherein said storage media comprise information storage tapes.

8. A system according to claim 6 wherein said information is a series of binary numbers.

9. A system according to claim 8 wherein said first and second signals are electrical representations of a binary numeral derived as described from said groups of storage media.

10. A system according to claim 6 wherein said first and second signals are a single binary digit.

References Cited in the file of this patent

UNITED STATES PATENTS

2,499,225	Marshall	Feb. 28, 1950
2,648,060	Turner	Aug. 4, 1953
2,942,238	Eckhardt et al.	June 21, 1960
2,978,676	Spencer	Apr. 4, 1961
3,004,253	Wilson	Oct. 10, 1961
3,009,134	Brosh	Nov. 4, 1961