Sabotage of Intruder Alarm System Loop

Karel Burda
burda@vut.cz
Brno University of Technology, Brno, Czech Republic

Summary
This article discusses the sabotage of loops of intruder alarm systems. Although loop alarm systems are now gradually being replaced by digital alarm systems, they are still significantly present in practice. This paper describes two experimentally verified techniques for sabotaging balanced loops. The first technique is based on the jump replacement of the balancing resistor by a fake resistor. The second technique is based on inserting a series-parallel combination of two rheostats into the loop. By alternately changing the resistance of these rheostats, a state is reached where the balancing resistor is shorted by the parallel rheostat and replaced by the series rheostat. Sabotage devices for both attacks are technically simple and inexpensive, so they can be made and used by an amateur. Owners of loop alarm systems should become find out about this threat.

Keywords:
Security, intruder alarm system, balanced loop, loop sabotage.

1. Introduction

The inventor of the first electrical alarm system was Mr. A. R. Pope, who patented it in 1853 [1]. The principle of this system is illustrated in Figure 1. In the doors and windows of the protected house, switches were installed. If an attacker opened such a door or window, the corresponding switch was switched on, the electrical circuit (called a loop) was closed and the electric bell began to ring. Later, the increasing number of loops in a single system necessitated the introduction of a central element called a control panel. The control panel evaluates the status of all the loops connected to it. If an attack is detected, the control panel signals this status (called an alarm) to the system owner. Bells, bulbs and sirens are used to signal an attack.

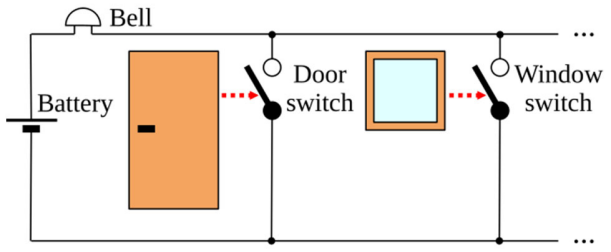

Fig. 1 The principle of the first intruder alarm system.

Until the 1970s, alarm systems did not change significantly. They were still loops with switching elements that switched on or off in response to the activities of an attacker. After the aforementioned door and window switches appeared pressure detectors and foil strips. By pressing the pressure detector (e.g. the attacker stepping on the doormat), the loop was switched on. The metal foil strips were used to detect the breakage of window panes. They were glued around the perimeter of the glass pane and an electric current flowed through them. The breaking of the pane broke the foil strip, thus breaking the loop. In the 1970s, the development of microelectronics allowed the use of non-mechanical processes to detect an attack too. The first detectors to appear were PIR sensors ("Passive Infrared Sensor"), which detected an attacker based on the infrared radiation of his body. Later on, glass-break detectors appeared, which detect the breaking of a window based on the sound of breaking glass.

Today, there are many different types of detectors that detect an attack based on various physical processes. When an attack is detected, the detector switches on or off its internal switch. By switching it on or off, the detector changes the magnitude of the current in the loop that connects it to the control panel. The control panel powers the loop and monitors the current in the connected loop. It can thus detect the state of the switch in the respective detector, i.e. it can determine whether the detector is in a quiescent state or has declared an alarm. Therefore, attackers naturally seek to prevent the control panel from being able to use the loop to detect the true state of the detector. This modification of loop behavior is called loop sabotage.

The alarm system has two modes of operation. When no one is supposed to be in the object, the system is in armed mode and the control panel signals the owner of the object with all alarm messages about intrusion into the object. Thus, an intruder cannot access the system cabling undetected. However, at times when persons may be in the object, the alarm system is switched to the unguarded mode and the control panel then ignores the detectors' messages about the entry and movement of persons. This time offers attackers opportunities to sabotage the loops. If the cabling is under the plaster, sabotage is complicated but still possible. However, when the cabling is located in the rails on the plaster (quite common), sabotage is relatively easy. Then, for example, a janitorial worker can sabotage the loops while cleaning the offices at night, paving the way for

Manuscript received July 5, 2023
Manuscript revised July 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.7.4

a later attack. Other opportunities for sabotaging loops are object modifications, interior renovations, etc.

This article discusses the possibilities of sabotaging loops of alarm systems. First, the functioning of loops is explained in detail and then two possible loop sabotage techniques are described and explained. The techniques suggested are very simple and therefore any handyman can prepare for and perform them. It should be still mentioned that loop alarm systems are currently being replaced by systems in which control panels communicate digitally with their detectors. On the other hand, loop systems are still in use to a significant extent. Due to the technical simplicity and ease of the described attacks, owners of loop systems should become find out about this threat. The point is that they should be able to assess the danger of this threat to their systems and respond adequately.

2. Loops for alarm systems

It has already been mentioned that the detector signals its status to the control panel via an internal switch. In the quiescent state, this switch is either on or off (e.g. [2], [3]). In the first case, current flows through the loop in the quiescent state and stops when an alarm occurs. This type of switch is abbreviated as NC ("Normally Closed"). In the second case, the detector switch is off in the quiescent state. The control panel recognizes this state by the fact that no current is flowing through the loop. On the other hand, when an alarm occurs, the switch will be on and current will flow through the loop. This type of switch is abbreviated NO ("Normally Open"). An example of a loop with a NO switch is at the top of Figure 2 and an example of a loop with an NC switch is at the bottom.

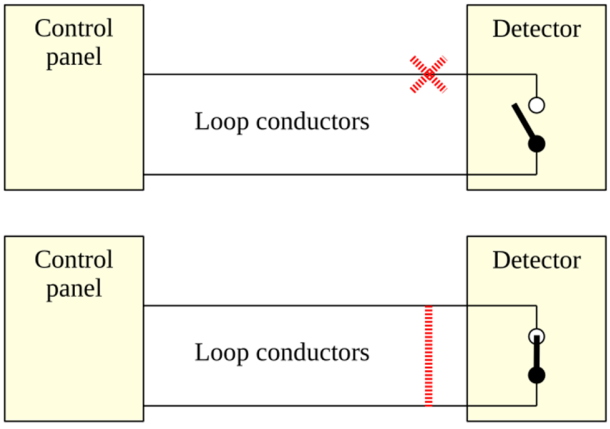

Fig. 2 Loop with NO switch (top) and NC switch (bottom).

The figure also indicates the attacker's options to prevent the control panel from detecting the true state of the switch in the detector. This type of attack is called loop sabotage. In the case of an NO switch, the attacker can break the loop conductor anywhere (marked with a red cross). Even if the detector then turns on its switch, no electrical current can flow through the loop and the control panel will therefore not recognize the alarm. In the case of the NC switch (lower part of the picture), an attacker can short-circuit both loop wires anywhere (indicated by the red line in the picture). Then, even if the detector turns off its switch, current will still flow through the loop at the control panel location and the control panel will again be unable to detect the alarm.

The types of sabotage described are both easy to perform and laborious to detect. Experts have therefore devised a variety of schemes to make possible sabotage more difficult (e.g., [3], pp. 78-87). However, the resulting solutions were technically and operationally complex. It was not until the 1990s that electronics became affordable, allowing the control panel to continuously measure loop resistance. In this case, the detectors are equipped with a balancing resistor R with resistance R. The control panel then detects the detector's quiescent state by measuring the loop resistance V, which corresponds to the value of R with a certain tolerance. This tolerance is enforced by practical circumstances such as manufacturing tolerances on the values of the balancing resistances R or different loop lengths. If we denote the lower or upper limit of the tolerated band by N or M, respectively, then formally it must be the case that $N \leq V \leq M$. The described solution is called a balanced loop and is often abbreviated as EOL ("End-of-line resistor loop"). In loop alarm systems, this type of loops is dominant.

The top of Figure 3 shows an example of a balanced loop with a NO switch and the bottom is a balanced loop with a NC switch. For both variants, the actual loop wiring is on the left and the loop state diagram is on the right. According to this diagram, the control panel determines the state of the connected detector based on the measured loop resistance V.

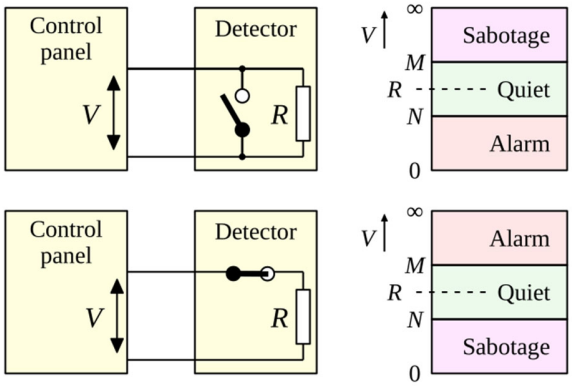

Fig. 3 Balanced loop with NO switch (top) and NC switch (bottom).

In both cases, the control panel continuously measures the resistance V of the loop. If $N \leq V \leq M$, then the control panel has confirmed that the detector is in a quiescent state (green bands in the state diagrams on the right). In the case of a loop with NO switch, if the detector detects an attack, it will turn its switch on, thus shorting the balancing resistor R. If we neglect the resistance of the loop conductors, then the value of the loop resistance V drops to zero. The control panel's decision about the detector state is simplified by the criterion that when the resistance V falls below the lower limit, i.e. $V < N$, an alarm is raised. When an attack is detected in the case of a loop with an NC switch, the switch opens and so, if the resistance of the wire insulation is neglected, the value of the resistance V approaches infinity. The control panel's criterion for an alarm in this case is that $V > M$. The states $V > M$ for NO switch or $V < N$ for NC switch is evaluated by the control panel as a loop sabotage. In the first case it is a loop sabotage by loop interruption and in the second case it is a loop sabotage by loop short circuit.

In the previous paragraph, the so-called simply balanced loop was described. For this, the detector contains one switch S and one resistor R. The control panel can then identify three possible states according to the value of the resistance V - quiet, alarm and loop sabotage. If more states need to be distinguished, a so-called multiple balanced loop is used. Very often a double balanced loop is used in the circuit shown in Figure 4.

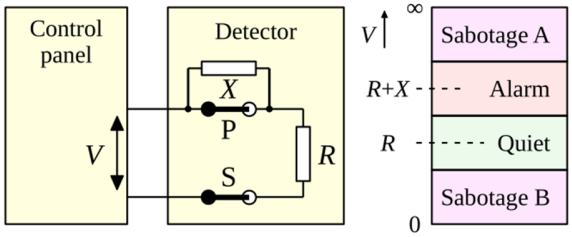

Fig. 4 Example of a double balanced loop.

In the above figure it can be seen that in addition to switch S and resistor R, switch P and resistor X with resistance X are also installed in the detector. Resistor X allows to define another band in the range of resistance values V. In the diagram above, this new band defines the alarm state. In the quiescent state, the S switch is closed. If an attacker removes the detector cover to change the detector settings, switch S will be opened. This event leads to loop disconnection and the declaration of a state called detector sabotage. In the quiescent state, both switches are closed, so the loop resistance $V = R$. This state is marked as green band in the diagram on the right. If the detector alarms, it opens switch P and the loop resistance rises to $V = R+X$ (marked as red band in the diagram on the right). If an attacker tries to remove the detector cover, switch S opens and the loop resistance V approaches infinity. This situation is interpreted by the control panel as a sabotage of the detector (marked as sabotage A in the diagram on the right). And if the attacker tries to short-circuit the loop, the value of V drops to zero and this event is presented as sabotage of the loop by short-circuit (marked as sabotage B in the diagram).

It is evident that a multi-balanced loop increases the number of events that the control panel is able to identify. However, it is still true that if the attacker, in any type of loop sabotage, ensures that the loop resistance value V is within the tolerated range between N and M, the sabotage will be successful.

The resistance value R of the balancing resistor is not standardized, and different systems are designed for different values. In most systems, resistors with values of R = 1 kΩ, 2.2 kΩ, 3.3 kΩ or 5.6 kΩ are used. As far as tolerance band values are concerned, these are rarely specified by manufacturers. In [4] on p. 43, it is stated, for example, that for R = 1 kΩ, must be valid that 0.8 kΩ ≤ V ≤ 1.5 kΩ. In [5], for R = 4.7 kΩ, it must hold that 3.2 kΩ ≤ V ≤ 6.4 kΩ (p. 21), and in [6] it is stated that for a given R, $V = R \pm 20\%$. All these values are valid for the case of a double balanced loop. Thus, from the above available data, it can be estimated that the usual lower limit N tends to be 70 to 85% of the value of R and the upper limit M is 110 to 150% of the same value.

3. Loop sabotage

In the publicly available literature, at most only the sabotages according to Figure 2, i.e., sabotages on unbalanced loops, are described (e.g., [2], [3], [7], [8]). The attack on a balanced loop is discussed only in [9] (p. 10). Specifically, it is an attack on a simply balanced loop by connecting in parallel a resistor B with resistance value $B = R$. In the referenced source, the author concludes that this sabotage is possible only for control panels with large tolerance. And he is right. In described case, the control panel detects a jump change of resistance from the value $V = R$ to the value $V = (B \cdot R)/(B+R) = R^2/(2 \cdot R) = R/2$. In order not to declare sabotage, it would have to be true for the lower bound N that $N \leq R/2$. However, such a large tolerance is not used in control panels.

This chapter describes two loop sabotage techniques. From a technical point of view, they are very simple and can be prepared and performed by any handyman. The first technique is based on the jump replacement of the balancing resistor R by a fake resistor R′. However, this simplest technique has the disadvantage of interrupting the current in the loop for a short time, which higher security control

panels may not tolerate. The second technique is somewhat more complex but universal.

The first sabotage technique is based on the jump replacement of the balancing resistor R by a fake resistor R′ of the same value. If the control panel of the alarm system is tolerant to short-term loop breaks, this sabotage technique will be successful. Experiments have shown that a conventional mechanical switch is often sufficient for successful switching. An electronic switch can be used to possibly reduce the switching time.

A schematic of the sabotage device and its connection to the loop is shown in Figure 5. The device consists of a switch S and a sabotage resistor B whose resistance B is equal to the resistance R of the loop balancing resistor R, i.e. $B = R$. The sabotage procedure is as follows. At the point of access to the cable, the conductors are stripped of insulation for a sufficient length and the sabotage device is connected to them. The device shall be connected to one conductor of the loop by means of clamps X and Y so that there is a sufficient gap between the two clamps to allow later breaking of the conductor. The other conductor is connected to the device using the Z clamp.

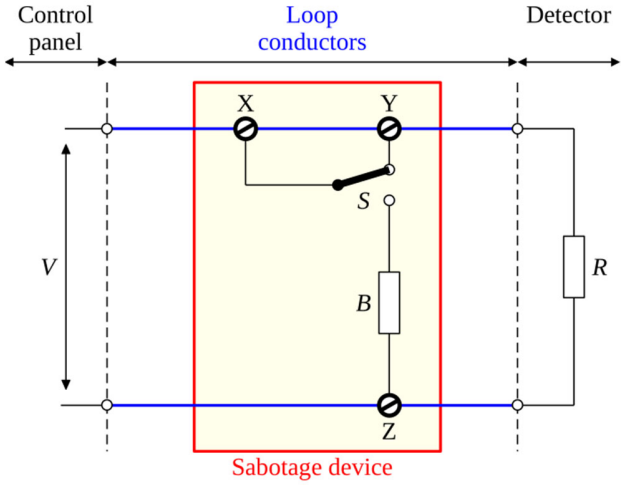

Fig. 5 Schematic of the sabotage device with invariable resistor.

Initially, the S switch is in the upper position as shown in the figure. Subsequently, the wire between clamps X and Y is cut, but since the X and Y clamps are connected by switch S, nothing has changed from the control panel's point of view. The loop resistance V is still equal to the correct value of R. Then switch S is switched to the down position, which disconnects the detector and replaces the balancing resistor R with the sabotage resistor B. Resistor B has the same resistance as resistor R and so the control panel is unable to detect any change other than a momentary loop break.

Then the two wires leading to the detector are cut and a fake resistor R′ with resistance $R' = R$ is connected to the ends of the wires at clamps Y and Z. Then the switch is switched back to the default position, thus the fake resistor R′ is now connected to the control panel. Since its resistance is the same as that of the original balancing resistor, the control panel has no reason to signal sabotage. Finally, the two ends of the cut wire between the X and Y clamps are connected, the sabotage device is disconnected from the line and the sabotage is masked. The control panel is now unable to determine the true status of the detector.

If the control panel does not tolerate short-term interruptions of the loop current, a second sabotage technique can be used. In this case, the sabotage device (see Figure 6) consists of two variable resistors A and B and one switch S. The device is connected to one loop conductor by clamps X and Y, so that there is a sufficient gap between the two clamps to cut the conductor later. The device is connected to the other conductor by clamp Z. At the start, the resistance of resistor A is set to zero, switch S is open and the resistance of resistor B is set to the specified value (see below).

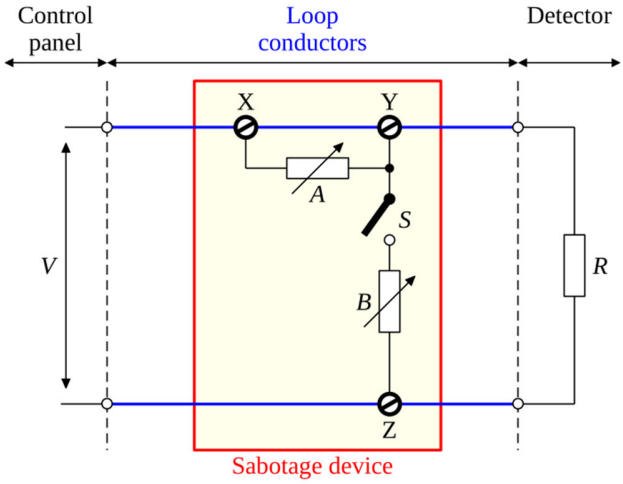

Fig. 6 Schematic of the sabotage device with rheostats.

A mathematical model is needed to explain this sabotage technique in more detail. In the model, relative resistance values are used, with the reference value being the value R of the balancing resistor R. Then the relative loop resistance $v = V/R$, the relative resistances of the variable resistors $a = A/R$ and $b = B/R$, respectively, and the relative resistance of the balancing resistor $r = R/R = 1$. The relative upper limit of the tolerance band is $m = M/R$ and the relative lower limit is $n = N/R$.

The other model parameters are the quantities e and d, which we call the upper and lower relative tolerance widths $e = m-1$ and $d = 1-n$, respectively (see also Figure 9).

Related to these is the parameter $\tau = d+e = m-n$, which is the relative total tolerance bandwidth of the control panel. That these are relative values can be seen from the small letter used to denote the quantity. Therefore, unless there is a risk of misunderstanding, the word "relative" will be omitted in the following. The sabotage proceeds in steps, which are indexed by the variable i, where the moment of initiation of the i-th step is denoted by the variable t_i and the values of the resistances a, b and v at these moments are denoted by a_i, b_i and v_i.

When the sabotage device is fully connected to the loop, the circuit as shown in Figure 7 is formed.

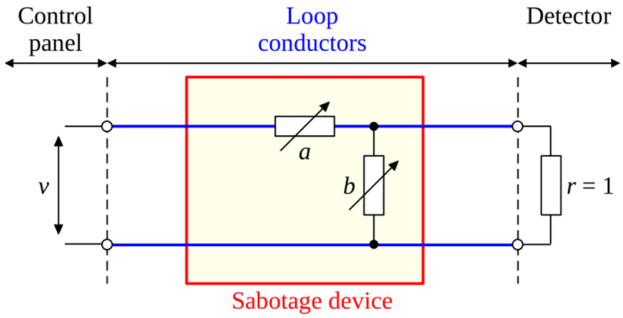

Fig. 7 Sabotage device in the loop.

In this circuit, resistor a with resistance value a_i is connected in series with a parallel combination of variable resistor b with value b_i and a balancing resistor with resistance value $r = 1$. The parallel combination of resistors b and r can be replaced by an equivalent resistor c with value c_i:

$$c_i = \frac{r \cdot b_i}{r + b_i} = \frac{b_i}{1 + b_i}. \qquad (1)$$

The above substitution leads to the circuit shown in Figure 8.

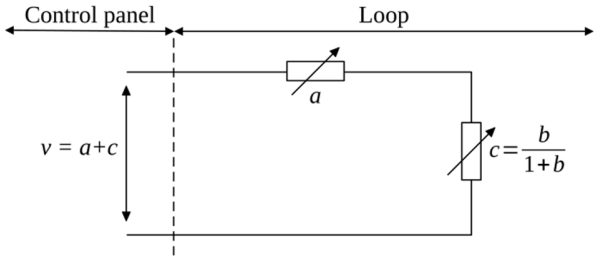

Fig. 8 Schematic of the equivalent loop.

For the total resistance v_i of this loop, the following relation holds:

$$v_i = a_i + c_i = a_i + \frac{b_i}{1 + b_i}. \qquad (2)$$

The principle of sabotage is that by repeatedly increasing the value of a followed by decreasing the value of b (and therefore also the value of c), the resulting loop resistance v is kept within the tolerance band $\langle n, m \rangle$. The value of a thus gradually approaches $r = 1$ and the value of b approaches zero. Eventually, a state is reached where $a = r = 1$ and where the balancing resistor r in the detector is shorted by the zero value of b. The detector can then be disconnected from the loop without the control panel declaring a sabotage.

At the beginning of the sabotage, the wire between clamps X and Y is unbroken, the resistance of resistor a is set to zero (i.e. $a_0 = 0$), switch S is open and the resistance of resistor b is set to b_0 (see below for details). At time t_0, switch S is turned on and a resistor of resistance b_0 is connected in parallel to resistor $r = 1$. This results in a jump reduction in the value of the loop resistance, with the requirement that no sabotage is declared. Thus, the following must be true:

$$v_0 = a_0 + \frac{b_0}{1 + b_0} \geq n = 1 - d. \qquad (3)$$

To reduce the value of v to the lower limit n of the tolerance band when $a_0 = 0$, the following must hold for b_0:

$$\frac{b_0}{1 + b_0} = 1 - d. \qquad (4)$$

The solution to this equation is the value:

$$b_0 = \frac{1 - d}{d}. \qquad (5)$$

So, if at the beginning of the sabotage the resistor b is set to this value, then according to relation (3) the switching of the switch S at time t_0 will cause a tolerated decrease of the loop resistance to the value $v_0 = 1-d = n$ (see Figure 9). And since $a_0 = 0$, this value is also the initial value c_0 of the resistance of the parallel combination of resistors b and r.

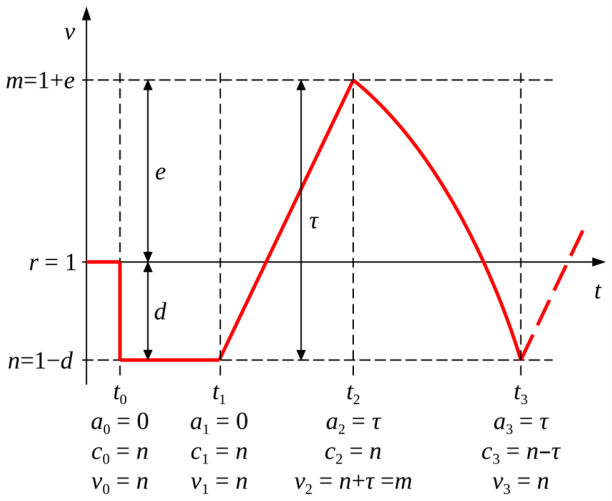

Fig. 9 The principle of sabotage with rheostats.

At time t_1, the wire between clamps X and Y is cut, thus inserting resistor a into the loop with $a_1 = a_0 = 0$. According to equation (2), this leaves the loop resistance v unchanged, i.e. $v_1 = v_0$. Subsequently, increasing the resistance value of the variable resistor a to $a_2 = \tau$ results in the loop resistance at time t_2 being $v_2 = v_1 + a_2 = n + \tau = m$. This means that the loop resistance v will be at the tolerated maximum of m. Then the value of b will start to decrease, which will also decrease the value of c. At time t_3 the above value will be reduced by the value of τ, so that at this point the loop resistance will be $v_3 = m - \tau = n$, i.e. the loop resistance will now be back at the tolerated minimum n. This is alternately continued.

It is now possible to explain the trajectory of the value v in the tolerance band in more detail. As already mentioned, the purpose of the sabotage device is to gradually increase the resistance a from 0 to $r = 1$ and decrease the resistance b from b_0 to 0. An example of the corresponding progression of changes in resistance a versus time is shown in Figure 10.

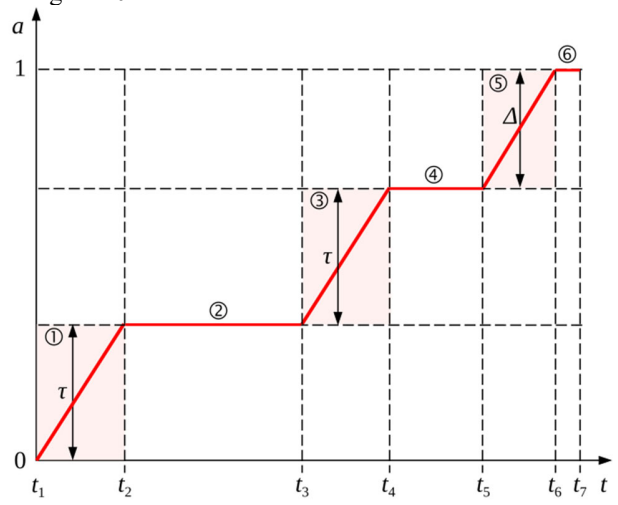

Fig. 10 Time course of resistance changes a.

In our example, the value of a is increased in three steps, indicated by the symbols 1, 3 and 5 (highlighted by a circle). The phase labeled 1 occurs at time interval t_1 to t_2 and during this phase the resistance a increases from $a_1 = 0$ to $a_2 = \tau$. In the interval t_2 to t_3, the value of b is changed and hence the value of c. The value of a remains unchanged, i.e. $a_3 = a_2$. The interval t_3 to t_4 is followed by phase 3, during which the resistance a_3 increases again by the value τ, i.e. to $a_4 = 2 \cdot \tau$. Then follows the interval t_4 to t_5, when the value of c is changed, so that in this interval the value of a will again be unchanged. Finally, in the interval t_5 to t_6, the phase 5 occurs, during which the resistance a finally reaches the target value $a_6 = 1$.

From the figure, it is clear that the increase Δ of the resistance a in this final phase is generally smaller than the value τ. For this residual resistance Δ, it is formally true that:

$$\Delta = 1 - K \cdot \tau\,, \tag{6}$$

where K is the number of times the resistance a is increased by value τ. For K, it is of course true that:

$$K = \left\lfloor \frac{1}{\tau} \right\rfloor, \tag{7}$$

where the notation $\lfloor x \rfloor$ represents the greatest integer less than or equal to x. In our example, $K = 2$.

An example of the time history of changes in resistance c is shown in Figure 11. As already mentioned, for this resistance the objective is to reduce its value from $n = 1 - d$ to 0.

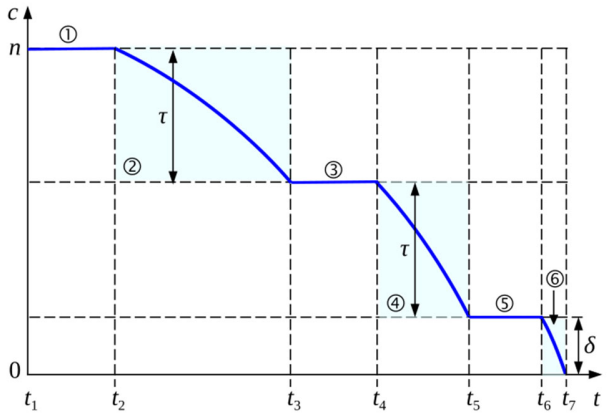

Fig. 11 Time course of resistance changes c.

In our example, the value of c decreases in three phases, which are denoted by the symbols 2, 4 and 6 (highlighted by a circle). Phase 2 takes place in the time interval t_2 to t_3 and during this phase the resistance c drops from $c_2 = n$ to $c_3 = n - \tau$. In the interval t_3 to t_4 the value of a is adjusted, therefore the value of c does not change in this interval, i.e. $c_4 = c_3$. In the interval t_4 to t_5, phase 4 takes place, during which the resistance c_4 drops again by the value τ, i.e. to the value $c_5 = n - 2 \cdot \tau$. In the interval t_5 to t_6 the value of a is again adjusted, so that in that interval the value of c is unchanged. Then, in the interval t_6 to t_7, phase 6 takes place, during which the resistance c finally reaches the target value $c_7 = 0$. The decrease δ of the resistance c in this final phase is generally smaller than the value of τ. For the value of this residual resistance δ, it is hold:

$$\delta = n - L \cdot \tau\,, \tag{8}$$

where L is the number of times the resistance c is decreased by value τ. For L, it is of course true that:

$$L = \left\lfloor \frac{n}{\tau} \right\rfloor, \tag{9}$$

where the notation $\lfloor x \rfloor$ represents the greatest integer less than or equal to x. In our example, $L = 2$.
The time courses in Figures 10 and 11 can now be used to piece together the resulting loop resistance v trajectory for our example. That trajectory is shown in Figure 12.

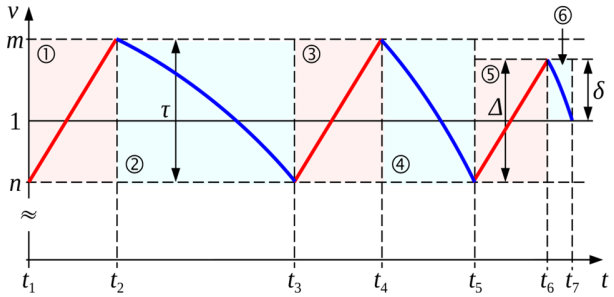

Fig. 12 Example of loop resistance trajectory during sabotage.

In practice, it is a sequencing of the above described phases 1 to 6 into a single sequence. This course starts at time t_1 with the values $a_1 = 0$ and $c_1 = n$, so that the resulting loop resistance $v_1 = a_1+c_1 = n$. In phase 1 the resistance a is increased by the value τ, so that at time t_2 it is true that $a_2 = \tau$ and $c_2 = n$. Then the loop resistance $v_2 = n+\tau = m$. This is followed by phase 2, during which the value of resistance c decreases by the value of τ. Thus, at time t_3, $a_3 = \tau$ and $c_3 = n-\tau$ and the value of $v_3 = n$. The same is true for phases 3 and 4, so that at time t_5 the values of the resistances $a_5 = 2\cdot\tau$ and $c_5 = n-2\cdot\tau$ and the resulting loop resistance $v_5 = a_5+c_5 = n$. At phase 5 the value of a is increased by the residual resistance Δ, so that $a_6 = 2\cdot\tau+\Delta = 1$, $c_6 = c_5 = n-2\cdot\tau$ and the loop resistance $v_6 = a_6+c_6 = n+\Delta$. Then, in phase 6, c is finally reduced by the residual resistance δ and so at time t_7, $a_7 = 1$ and $c_7 = c_6-\delta = (n-2\cdot\tau)-\delta = n-(2\cdot\tau+\delta) = n-n = 0$. The final value of the loop resistance $v_7 = a_7+c_7 = 1 = r$.

The trajectory described above is just one particular case. In general, the trajectory of the resistance v starts at time t_1 at value n, followed by K rises of the resistance v by the value τ, which are interspersed with L drops by the value τ. Then, this is followed by a rise in resistance v of value Δ together with a fall of value δ. The order of this final rise or fall depends on the values of K and L. If $K = L$, the first process is the final rise, which is followed by the final fall. An example of this trajectory is shown in Figure 12, where $K = L = 2$. However, in the case of $K = L+1$, the first is a final fall followed by a final rise. An example of this variation for $K = 2$ and $L = 1$ is shown in Figure 13.

The attacker alternately increases the resistance a and then decreases the value of the resistance c so as to keep the loop resistance v within the tolerance band $\langle n, m\rangle$. It uses the pre-established marks on the rheostat scales to do this. In this way, the value of resistance a is gradually approached to the value of resistance $r = 1$ and the value of resistance c is approached to zero. Eventually, a state is reached where $a = r = 1$ and where the balancing resistor R in the detector is short-circuited by the zero value of b. Then the detector and its balancing resistor can be cut off from the line without the control panel reporting sabotage. The attacker will connect a false resistor R′ of resistance R to the cut wires at clamps Y and Z and reverse the procedure to return to the initial state, i.e. to the state when $a = 0$ and $b = b_0$. Finally, the attacker connects the two ends of the cut wire between clamps X and Y, disconnects the sabotage device and masks the sabotage appropriately.

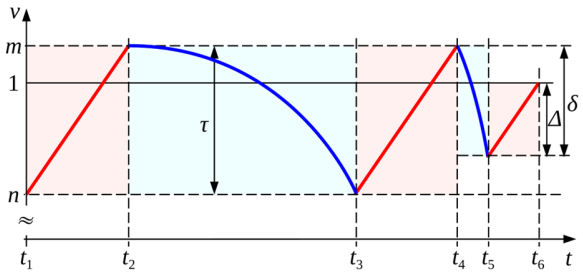

Fig. 13 Example of a loop resistance trajectory for $K \neq L$.

Now a few words about the possibility of improving the sabotage device with rheostats. From Figure 11 it is clear that the resulting resistance c of the parallel combination of b and r drops very steeply towards the end of the sabotage. At this stage, then, a small error in adjusting the position of the rheostat B can cause the sabotage to be declared. To minimize this risk, it is advisable to use a logarithmic rheostat instead of a linear one. The normalized resistance b of the linear and logarithmic rheostat is shown in Figure 14. The horizontal axis of the graph shows the values of the variable $x \in \langle 0, 1\rangle$, which is the actual distance of the rheostat slider from the start of the resistance path relative to the total length of the rheostat resistance path. The course of resistance b is shown in blue for a linear rheostat and in purple for a logarithmic rheostat.

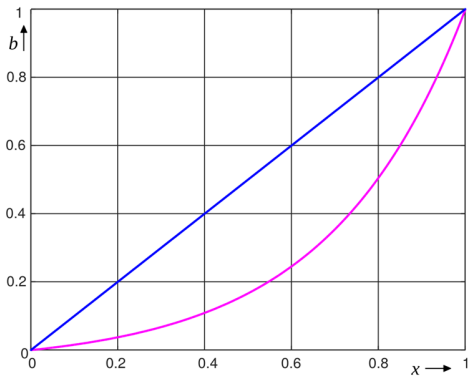

Fig. 14 Course of resistance b for linear (blue) and logarithmic (purple) rheostat.

Logarithmic rheostats are called logarithmic because the logarithm of their resistance versus the value of x is practically a straight line. The resistance is therefore given by the exponential equation $b = w^x$, where w is the maximum value of the resistance of the rheostat. The problem with this equation, however, is that for $x = 0$ the resistance b comes out non-zero, which is contrary to physical reality. Therefore, various approximations are used, and the following is used in this paper:

$$b = \frac{w^x - 1}{w - 1}, \text{where } w = \left(\frac{1-p}{p}\right)^2. \qquad (10)$$

The above approximation contains the exponential term w^x and also satisfies the requirement that for $x = 0$, $b = 0$ and for $x = 1$, $b = w$. The parameter p is the relative resistance of the rheostat at the midpoint of its path (i.e., the value of b for $x = 0.5$). Most manufacturers produce rheostats with a value of p in the interval ⟨0,15, 0,2⟩ (e.g., [10], p. 85). In the following, the value of $p = 1/6$ is used, so that $w = 25$.

The resistance dependence of the parallel combination of the resistors b and r, i.e. the course of the resulting relative resistance c, is shown in Figure 15 for both types of rheostats. The blue curve is for a linear rheostat and the purple curve is for a logarithmic rheostat. The curves are for slider positions from $x = 1$ (i.e., maximum resistance value) to $x = 0$ (i.e., zero resistance). From the figure it is clear that the purple dependence is almost linear in nature, so in the sabotage device it is preferable to use a rheostat with a logarithmic course for resistor B.

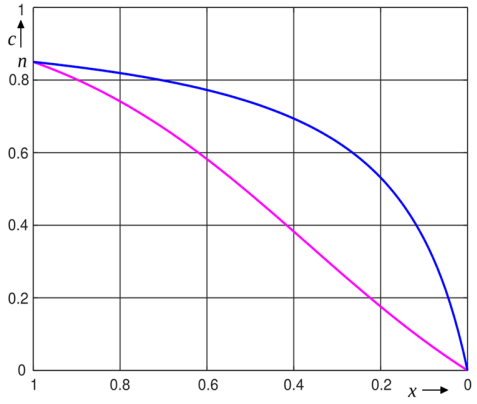

Fig. 15 Relative resistance c for linear (blue) and logarithmic (purple) rheostat.

Another possible improvement of the sabotage device with rheostats consists in replacing mechanical rheostats with digital ones. The resistance of this type of rheostat can be adjusted electronically in k steps, where typically $k = 128$ or 256 (e.g. [11]). The device could then be controlled by a simple processor, thus achieving higher accuracy and at the same time a higher sabotage speed. It would also be possible to sabotage loops in control panels with extremely narrow tolerance band τ. Figure 16 shows a possible dependence of loop resistance changes v for the case where the relative resistances of the rheostats $a = 1$, $b = 19$, and the numbers of rheostat steps are $k_a = 128$ and $k_b = 256$.

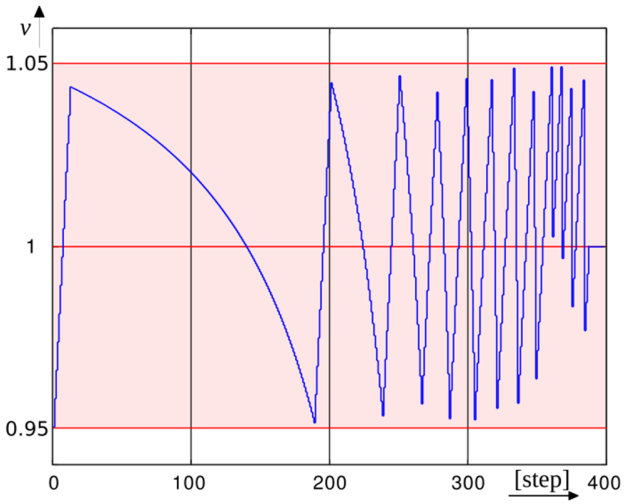

Fig. 16 Loop resistance trajectory for a device with digital rheostats.

In the above example, the loop resistance remains within the range of values $v = 1 \pm 0.05$ (red highlighted area). Even if the control panel had such an extremely narrow tolerance band (i.e. ± 5%), the sabotage would have been successful. It is also worth noting that the relative resistance in the loop is often only close to the limits of $m = 1.05$ and $n = 0.95$ compared to Figures 12 or 13. This is due to the fact that the resistance of digital rheostats can only be changed discretely and not continuously.

4. Conclusions

In the beginning of the article the problem of loop alarm systems is discussed. Although this type of systems is gradually being replaced by digital alarm systems, it is still true that loop systems are widely used in practice. The main topic of the paper is the attack on loop systems by so-called sabotage of loop. In the publicly available literature, only sabotages targeting simple loops are widely published. However, practically applicable sabotages targeting balanced loops, which are quite dominant in practice, are not published. Thus, owners of loop alarm systems can quite reasonably assume that if they use balanced loops, their system is not vulnerable to the type of attack mentioned.

Two techniques for sabotaging balanced loops are described in this paper. The first technique is based on the jump substitution of a balancing resistor R by a fake resistor R′ of the same resistance (see Figure 5). The disadvantage

of this technique is short-term loop breakage, which higher security level control panels may not tolerate.

From this point of view, the second technique is quite general. In fact, control panels must respect the reality that, for practical reasons, the loop resistance can range from some minimum limit *N* to a maximum limit *M*. As part of the sabotage, a series-parallel combination of rheostats is inserted into the loop (see Figure 6). Initially, the resistance of the series rheostat is zero and the resistance of the parallel rheostat is sufficient so that the resulting loop resistance does not fall below a minimum limit of *N*. By increasing the resistance of the series rheostat, which is alternated by decreasing the resistance of the parallel rheostat, the resulting loop resistance is kept within the limits of *N* and *M*. The ultimate goal is a state where the parallel rheostat short-circuits the balancing resistor R in the detector and its role in the loop is taken over by the series rheostat.

To perform both of the above sabotages, the attacker must have access to the loop wires. The wires are most often routed either under plaster or in rails. If the wires are routed under plaster, sabotage is more difficult but still possible. Conductors routed in rails are more easily accessible and so the risk of loop sabotage will be much higher with such systems.

From the description of both sabotage techniques, it is clear that the devices needed are technically simple and cheap. Even an amateur can make and use them. Alarm system owners should therefore learn about this threat so that they can assess its danger to their system. Unfortunately, however, it is difficult to respond to this threat. In particular, the second of the sabotage techniques is virtually undetectable because it does not break the loop. Moreover, it can work even in control panels with an extremely narrow tolerance band (see Figure 16). Possible protections consist of making access to the loop conductors more difficult and monitoring the loop paths, for example by means of inspections, vibration detectors and camera systems. However, all these protections are only partial. The migration to a digital alarm system is a completely principled solution. If such a digital system is well cryptographically secured, any sabotage of the control panel's communication with its detectors is practically excluded.

References

[1] Pope A. R.: Improvement in electro-magnetic alarms. Patent US9802A, United States Patent Office, Washington 1853. https://patents.google.com/patent/US9802?oq=9802
[2] Honey G.: Intruder alarms. Elsevier, Oxford 2007.
[3] Trimmer H. W.: Understanding and servicing Alarm systems. Butterworth-Heinemann, Oxford 1999.
[4] -: MAXPRO Intrusion Series. Integrated Security Systems. Installation and Setup Guide. Honeywell, Runcorn 2021. https://bit.ly/3Km47nr
[5] -: ATS control panel. Installation guide. GE Security, Boston 2007. https://bit.ly/40KYXqI
[6] -: JA-116H BUS expander. Jablotron, Jablonec nad Nisou. https://bit.ly/3MaKMqG
[7] Hammer C.: Expedient B and E: Tactics and Techniques for Bypassing Alarms and Defeating Locks. Paladin Press, Boulder 1992.
[8] Garcia M. L.: The Design and Evaluation of Physical Protection Systems. Butterworth-Heinemann, Oxford 2008.
[9] Yeager W. B.: Techniques of Burglar Alarm Bypassing. Loompanics, Port Townsend 1990.
[10] -: Potentiometer PC-16. Datasheet. Piher Sensors & Controls, Tudela. https://bit.ly/40udRBG
[11] -: MCP41HVX1. Datasheet. Microchip Technology, Chandler 2013. https://bit.ly/3nLk5ih

Karel Burda received the M.S. and Ph.D. degrees in Electrical Engineering from the Liptovsky Mikulas Military Academy in 1981 and 1988, respectively. During 1988-2004, he was a lecturer in two military academies. At present, he works at Brno University of Technology. His current research interests include the security of information systems and cryptology.