

Sabotáž smyčky poplachového zabezpečovacího systému

Intruder alarm system loop sabotage

Karel Burda

burda@vut.cz

Fakulta elektrotechniky a komunikačních technologií VUT v Brně

DOI: -

Abstract: The subject of this article is sabotage of intruder alarm loops. Although this type of systems is gradually being replaced by digital alarm systems, it is still true that loop systems are significantly represented in practice. In this paper, two experimentally verified balanced loop sabotage techniques are described. The first technique is based on the stepwise replacement of the loop balancing resistor by a dummy resistor. The second technique is based on inserting a series-parallel combination of potentiometers into the loop. By alternately changing the resistance of these potentiometers, a condition is reached where the parallel potentiometer short-circuits the balancing resistor and the series potentiometer replaces the balancing resistor. Sabotage devices for both attacks are technically simple and cheap. Even an amateur can make and use them. Owners of loop alarm systems should learn about this threat.

Sabotáž smyčky poplachového zabezpečovacího systému

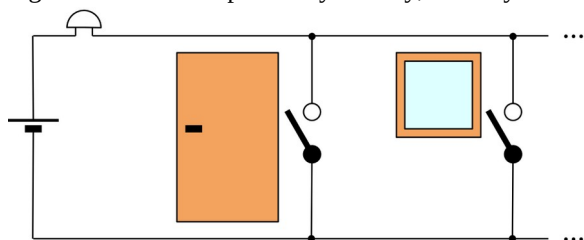
Karel Burda

Fakulta elektrotechniky a komunikačních technologií VUT v Brně
Email: burda@vut.cz

Abstrakt – Předmětem článku jsou sabotáže smyček poplachových zabezpečovacích systémů. Uvedený typ systémů je sice postupně nahrazován digitálními poplachovými systémy, avšak stále platí, že smyčkové systémy jsou v praxi významně zastoupeny. V článku jsou popsány dvě experimentálně ověřené techniky sabotáže vyvážených smyček. První technika je založena na skokové náhradě vyvažovacího rezistoru smyčky falešným rezistorem. Druhá technika spočívá ve vložení sériově paralelní kombinace potenciometrů do smyčky. Střídavými změnami odporu těchto potenciometrů se dosáhne stav, kdy paralelní potenciometr zkratuje vyvažovací rezistor a sériový potenciometr vyvažovací rezistor nahradí. Sabotážní přípravky pro oba útoky jsou technicky jednoduché a laciné. Zhotovit je a použít, zvládne i amatér. Majitelé smyčkových poplachových systémů by se o této hrozbě měli dozvědět.

1 Úvod

Vynálezcem prvního elektrického zabezpečovacího systému byl pan A. R. Pope, který si jej patentoval v roce 1853 [1]. Princip zmíněného systému ilustruje obrázek 1. U křídel vnějších dveří a oken chráněného domu se nacházely spínače, které byly v klidovém stavu rozepnuty. Pokud útočník takové dveře, nebo okno otevřel, tak došlo k sepnutí příslušného spínače, uzavřel se elektrický obvod a zvonek začal zvonit. Pozdější zvětšování počtu smyček v jednom systému si vynutilo zavedení centrálního prvku, který se nazývá ústředna. Ústředna vyhodnocuje stav připojených smyček a v případě detekce útoku tento stav (tzv. poplach) majiteli systému signalizuje. Pro signalizaci útoku se používaly zvonky, žárovky a sirény.



Obrázek 1: Princip prvního zabezpečovacího systému.

Až do 70. let minulého století se zabezpečovací systémy významně nezměnily. Stále se jednalo o smyčky se spínacími prvky, které sepnutím, resp. rozepnutím reagovaly na aktivitu útočníka. Po již zmíněných dveřních a okenních spínačích se objevily nášlapné detektory a fóliové proužky. Sešlápnutím nášlapného detektoru (například v rohožce) došlo k sepnutí smyčky. A kovové fóliové proužky sloužily k detekci rozbití okenní tabule. Lepily se po obvodu skleněné tabule a v klidovém stavu jimi protékal elektrický proud. Rozbitím tabule došlo k přetržení proužku fólie a tím k rozpojení smyčky.

dovém stavu jimi protékal elektrický proud. Rozbitím tabule došlo k přetržení proužku fólie a tím k rozpojení smyčky.

V 70. letech 20. století dovolil rozvoj mikroelektroniky používat k detekci útoku také jiné děje než-li mechanické. Jako první se objevily detektory PIR („Passive Infrared Sensor“), které detekovaly útočníka na základě infračerveného záření lidského těla. Později se objevily detektory tříštění skla, které detekují rozbití okna na základě zvuku rozbíjeného skla.

Dnes již existuje celá řada různých typů detektorů, které detekují útok na základě různých fyzikálních dějů. Při detekci útoku detektor sepne, resp. rozepne svůj interní spínač. Jeho sepnutím, resp. rozepnutím změní detektor velikost proudu ve smyčce, která jej s ústřednou spojuje. Ústředna smyčku napájí a velikost proudu v připojené smyčce sleduje. Dokáže tak zjistit stav přepínače v příslušném detektoru, tj. dokáže zjistit, zda je detektor v klidovém stavu, či vyhlásil poplach. Útočníci proto začali zcela přirozeně usilovat o to, aby ústředna nebyla schopna pomocí smyčky skutečný stav detektoru zjistit. Takováto úprava chování smyčky se nazývá sabotáž smyčky.

Poplachový systém má dva režimy provozu. Když se v objektu nemá nikdo nacházet, tak je systém v režimu zastřeženo a ústředna poplachová hlášení detektorů o vniknutí do objektu signalizuje majiteli. Ke kabeláži systému se tak útočník nemůže dostat nepozorovaně. Avšak v době, kdy se v objektu smí osoby nacházet, je poplachový systém přepnut do režimu odštěženo a ústředna hlášení detektorů o vstupu a pohybu osob ignoruje. Tato doba útočníkům nabízí příležitosti k sabotování smyček. Pokud se kabeláž nachází pod omítkou, tak je sabotáž komplikovaná. Avšak když je kabeláž umístěna v lištách na omítce (docela častý případ), tak je sabotáž relativně snadná. Potom například pracovník úklidové firmy může při nočním úklidu kanceláří sabotovat smyčky a připravit si tak cestu pro pozdější útok. Další příležitosti pro sabotáž smyček jsou stavební úpravy objektu, renovace interiéru apod.

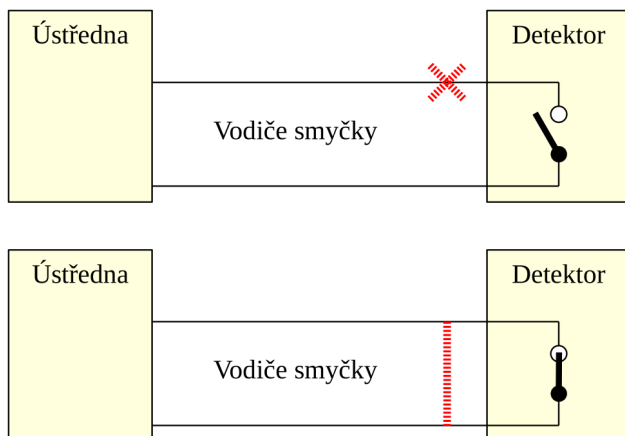
V tomto článku jsou diskutovány možnosti sabotáže smyček poplachových systémů. Nejprve je podrobně vysvětlena problematika fungování smyček a poté jsou popsány a vysvětleny dvě možné techniky sabotáže smyček. Navrhované sabotážní techniky jsou z technického hlediska velmi snadné a je schopen se na ně připravit a následně provést každý kutil.

Ohledně sabotáže smyček je ještě vhodné zmínit, že v současné době jsou smyčkové poplachové systémy nahrazovány systémy, v nichž ústředny se svými detektory komunikují digitálně. Na druhou stranu však platí, že smyčkové systémy jsou ve významné míře stále provozovány. Vzhledem k technické jednoduchosti a láci popisovaných útoků by se majitelé smyčkových systémů měli o praktické proveditelnosti zmíněných sabotáží dozvědět. Jde o to, aby nebezpečí této hrozby pro své systémy mohli posoudit a adekvátně na ni zareagovat.

2 Smyčky poplachových systémů

Již bylo uvedeno, že detektor signalizuje ústředně svůj stav pomocí spínače. V klidovém stavu je tento spínač buď sepnutý, nebo rozepnutý (např. [2], [3]). V prvním z uvedených případů pak v klidovém stavu protéká proud a při poplachu proud zanikne. Tento typ spínače se označuje zkratkou NC („Normally Closed“). V případě, kdy je spínač detektoru v klidovém stavu rozepnutý, ústředna tento klidový stav pozná podle toho, že smyčkou proud neprotéká. Naopak při poplachu dojde k sepnutí spínače a proud začne smyčkou protékat. Tento typ spínačů se označuje zkratkou NO („Normally Open“).

Příklad smyčky se spínačem typu NO vidíme na obrázku 2 nahoře a dole je příklad smyčky se spínačem NC. Na obrázku jsou naznačeny i možnosti útočníka, jak ústředně znemožnit zjištění aktuálního stavu spínače v detektoru. Tento typ útoku se nazývá sabotáž smyčky. V případě horního obrázku může útočník kdekoli přerušit vodič smyčky (označeno červeným křížkem). I když pak detektor svůj spínač sepně, tak smyčkou protékat elektrický proud nemůže a ústředna proto nepozná vyhlášení poplachu. V případě spínače NC (dolní část obrázku) může útočník oba vodiče smyčky kdekoli zkratovat (na obrázku naznačeno červenou čarou). Potom, i když detektor svůj spínač rozepne, tak v místě ústředny bude smyčkou protékat proud i nadále a ústředna opět není schopna vyhlášení poplachu detekovat.

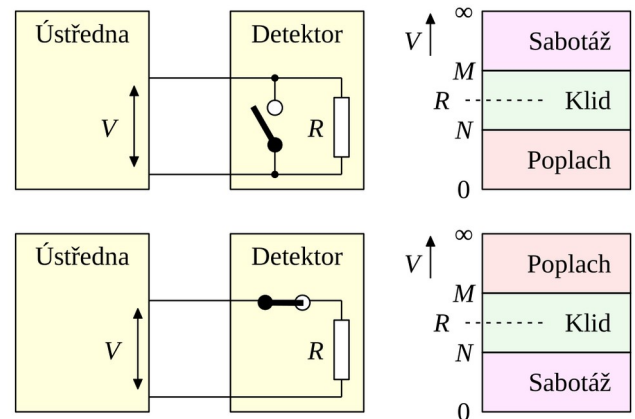


Obrázek 2: Smyčka se spínačem typu NO (nahore) a se spínačem typu NC (dole).

Popsané typy sabotáže jsou velmi snadné a pracně se zjišťují. Odborníci proto vymysleli celou řadu zapojení, která měla za úkol případnou sabotáž ztížit (např. [3], s. 78-87). Výsledná řešení však byla technicky a provozně složitá. Až v 90. letech minulého století se stala cenově dostupnou elektronika, která ústředně umožňuje průběžně měřit odpor smyčky. Detektory jsou v tomto případě kromě spínače vybaveny ještě tzv. vyvažovacím rezistorem R o odporu R . Klidový stav detektoru pak ústředna zjistí tak, že ve smyčce změří odpor V , který s určitou tolerancí odpovídá hodnotě R . Zmíněná tolerance je vynucena praktickými okolnostmi, jako jsou výrobní tolerance hodnot vyvažovacích odporů R nebo různá délka smyček. Pokud dolní, resp. horní hranici tolerovaného pásma označíme N , resp. M , tak formálně musí platit, že $N \leq V \leq M$.

Popsané řešení se nazývá vyvážená smyčka a často se označuje zkratkou EOL („End-of-line resistor loop“). Uvedený typ smyček je u smyčkových poplachových systémů v současné době dominantní.

V horní části obrázku 3 je uveden příklad vyvážené smyčky s NO spínačem a dole je vyvážená smyčka s NC spínačem. Pro obě varianty je vlevo samotné zapojení smyčky a vpravo je diagram, podle kterého ústředna hodnotám odporu V přiřazuje stavy detektoru.

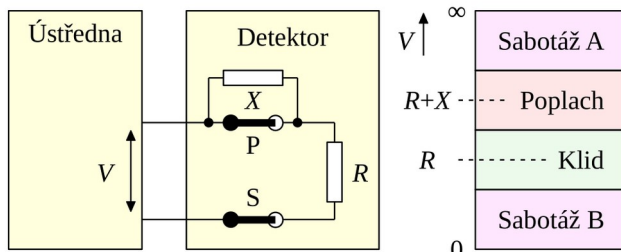


Obrázek 3: Vyvážená smyčka se spínačem NO (nahore) a spínačem NC (dole).

V obou případech ústředna průběžně měří odpor V smyčky. Pokud $N \leq V \leq M$, tak má ústředna potvrzeno, že detektor se nachází v klidovém stavu (zelená pásma na diagramech vpravo). Když pak v případě smyčky se spínačem NO detektor detekuje útok, tak svůj spínač sepně, čímž vyvažovací rezistor R zkratuje. Zanedbáme-li měrný odpor vodičů, pak hodnota odporu V smyčky klesne k nule. Rozhodování ústředny o stavu detektoru se zjednodušuje kritériem, že když odpor V poklesne pod dolní hranici, tj. $V < N$, tak je vyhlášen poplach. U smyčky se spínačem NC se při detekci útoku spínač rozepíná a tak, pokud zanedbáme izolační odpor, potom hodnota odporu V se blíží nekonečnu. Kritériem ústředny pro vyhlášení poplachu je v tomto případě skutečnost, že $V > M$. Stav $V > M$ u NO spínače, resp. $V < N$ u NC spínače, ústředna vyhodnocuje jako sabotáž smyčky. V prvním případě jde o sabotáž smyčky jejím přerušením a ve druhém případě se jedná o sabotáž zkratem smyčky.

V předešlém odstavci byla popsána tzv. jednoduše vyvážená smyčka. Pro ni platí, že detektor obsahuje jeden spínač S a jeden rezistor R . Ústředna pak podle hodnoty odporu V může identifikovat tři možné stavy – klid, poplach a sabotáž smyčky. Pokud je zapotřebí u detektoru rozlišit více stavů, tak se používá tzv. vícenásobně vyvážená smyčka. Velmi často se používá dvojité vyvážená smyčka v zapojení podle obrázku 4. Na zmíněném obrázku je vidět, že do detektoru je navíc nainstalován ještě spínač P a rezistor X o odporu X . Rezistor X dovoluje ve škále hodnot odporu V stanovit další pásmo hodnot, které v tomto případě definuje poplachový stav. Stav spínače S závisí na tom, zda útočník sejme kryt detektoru s cílem upravit chování detektoru. Tato událost vede k rozepnutí spínače a k vyhlášení stavu, který se označuje jako tzv. sabotáž detektoru.

V klidovém stavu jsou oba spínače sepnuty, takže odpor smyčky $V = R$. Pokud detektor vyhlásí poplach, tak rozeptne spínač P a odpor smyčky stoupne na hodnotu $V = R + X$. Pokud se útočník pokusí sejmut viko detektoru, tak se rozeptne spínač S a hodnota odporu smyčky V se blíží nekonečnu. Tuto situaci ústředna interpretuje jako sabotáž detektoru (na diagramu vpravo označeno jako sabotáž A). A pokud se útočník pokusí smyčku zkratovat, tak hodnota V klesne k nule a tato událost je prezentována jako sabotáž smyčky zkratem (na obrázku označeno jako sabotáž B). Je evidentní, že vícenásobně vyvážená smyčka zvyšuje počet událostí, které je schopna ústředna identifikovat. Stále však platí, že pokud se při libovolném typu sabotáže smyčky zajistí, aby hodnota odporu smyčky V se nacházela v tolerovaném pásmu mezi hodnotami N a M , tak sabotáž bude úspěšná.



Obrázek 4: Příklad zapojení dvojité vyvážené smyčky.

Hodnota odporu R vyvažovacího rezistoru není standardizována a různé systémy jsou konstruovány pro různé hodnoty. Ve většině systémů se používají rezistory o hodnotách $R = 1 \text{ k}\Omega$, $2,2 \text{ k}\Omega$, $3,3 \text{ k}\Omega$ nebo $5,6 \text{ k}\Omega$. Co se týká hodnot tolerančního pásma, tak tyto údaje výrobci uvádějí málokdy. V [4] na s. 43 se uvádí, že například pro $R = 1 \text{ k}\Omega$ musí pro odpor V smyčky platit, že $0,8 \text{ k}\Omega \leq V \leq 1,5 \text{ k}\Omega$. V systému [5] musí pro $R = 4,7 \text{ k}\Omega$ platit, že $3,2 \text{ k}\Omega \leq V \leq 6,4 \text{ k}\Omega$ (s. 21) a v [6] je stanoveno, že pro dané R musí být $V = R \pm 20\%$. Všechny tyto hodnoty platí pro případ dvojité vyvážené smyčky. Z výše uvedených dostupných údajů tak lze odhadnout, že obvyklá dolní hranice N bývá 70 až 85 % hodnoty R a horní hranice M činí 110 až 150 % téže hodnoty.

3 Sabotáž smyčky

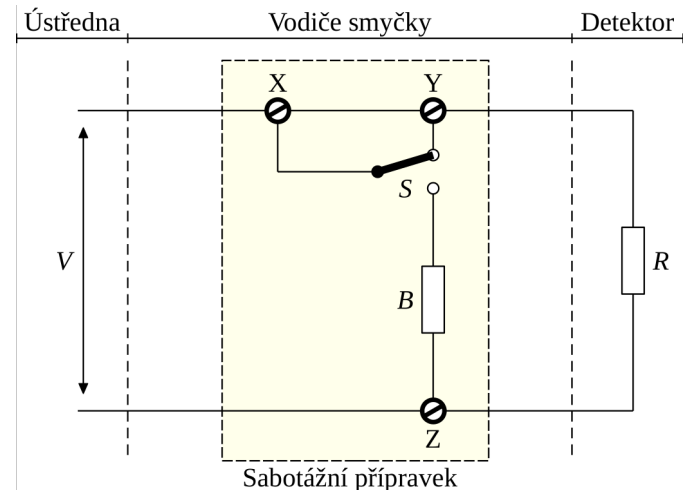
Ve veřejně dostupné literatuře jsou nejvýše popisovány pouze sabotáže na nevyvážené smyčky (např. [2], [3], [7], [8]). Útok na vyváženou smyčku je diskutován pouze v [9] (s. 10). Konkrétně se jedná o útok na jednoduše vyváženou smyčku paralelním připojením rezistoru B o hodnotě odporu $B = R$. Autor v odkazovaném prameni dochází k závěru, že popsaná sabotáž je možná pouze u ústředny s velkou tolerancí. A má pravdu. Ústředna totiž v daném případě zjistí skokovou změnu odporu z hodnoty $V = R$ na hodnotu $V = (B \cdot R) / (B + R) = R^2 / (2 \cdot R) = R/2$. Aby nebyla vyhlášena sabotáž, tak by pro dolní hranici N muselo platit, že $N \leq R/2$. Tak velká tolerance se však v moderních ústřednách nepoužívá.

V této kapitole jsou popsány dvě techniky sabotáže smyčky. Z technického hlediska jsou velmi jednoduché a zvládne se na ně připravit a provést je každý šikovnější kutil. První technika je založena na skokové náhradě vyvažovacího rezistoru R

falešným rezistorem B. Jde o nejjednodušší techniku, avšak její nevýhodou je krátkodobé přerušení proudu ve smyčce, které ústředny s vyšší úrovní bezpečnosti nemusí tolerovat. Druhá technika je poněkud složitější, avšak použitelná pro jakoukoliv smyčkovou ústřednu.

První sabotážní technika je založena na skokové náhradě vyvažovacího rezistoru R falešným rezistorem B o téže hodnotě. Pokud je ústředna zabezpečovacího systému tolerantní ke krátkodobému přerušení smyčky, tak tato technika sabotáže bude úspěšná. Experimenty ukázaly, že k úspěšnému přepnutí postačí běžný mechanický přepínač. Pro případné zkrácení doby přepnutí je možné použít elektronický přepínač.

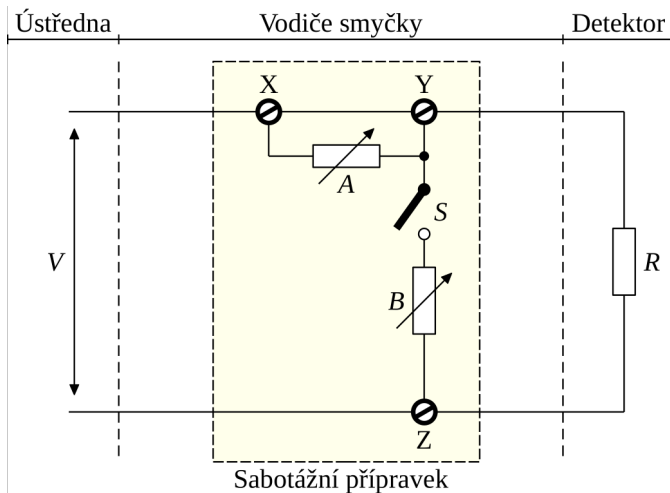
Schéma sabotážního přípravku a jeho napojení ke smyčce ilustruje obrázek 5. Přípravek sestává z přepínače S a ze sabotážního rezistoru B, jehož odpor B je roven odporu R vyvažovacího rezistoru R smyčky, tedy $B = R$. Postup sabotáže je následující. V místě přístupu ke kabelu se vodiče v dostatečné délce zbaví izolace a připojí se na ně sabotážní přípravek. Svorkami X a Y je přípravek připojen k jednomu vodiči smyčky takovým způsobem, aby mezi oběma svorkami byla dostatečná mezera potřebná k pozdějšímu přestřižení vodiče. Svorkou Z je přípravek připojen ke druhému z vodičů.



Obrázek 5: Schéma sabotážního přípravku s přepínačem.

Na počátku je přepínač S v horní poloze tak, jak uvádí obrázek. Následně je přestřižen vodič mezi svorkami X a Y, ale protože svorky X a Y přepínač S propojuje, tak z hlediska ústředny se nic nezměnilo. Odpor V smyčky je dále roven korektní hodnotě R . Poté je přepínač S přepnut do dolní polohy, čímž dojde k odpojení detektoru a k náhradě vyvažovacího rezistoru R sabotážním rezistorem B. Rezistor B má stejný odpor jako rezistor R a tak ústředna není kromě krátkodobého přerušení smyčky schopna detekovat jinou změnu. Následně se oba vodiče vedoucí k detektoru přestřihnou a ke koncům vodičů se u svorek Y a Z připojí falešný rezistor R' o odporu $R' = R$. Poté se přepínač přepne zpět do výchozí polohy, čímž se k ústředně nyní připojí falešný rezistor. Protože jeho odpor je stejný jako je odpor původního vyvažovacího rezistoru, tak ústředna nemá důvod signalizovat sabotáž. Nakonec se oba konce přestřiženého vodiče mezi svorkami X a Y propojí, sabotážní přípravek se od vedení odpojí a sabotáž se zamaskuje. Ústředna nyní není schopna zjistit skutečný stav detektoru.

Pokud ústředna krátkodobá přerušení smyčkového proudu netoleruje, tak je možné použít druhou sabotážní techniku. Sabotážní přípravek (viz obrázek 6) v tomto případě sestává ze dvou proměnných rezistorů A a B a z jednoho spínače S . Svorkami X a Y je přípravek připojen k jednomu vodiči smyčky tak, aby mezi oběma svorkami byla dostatečná mezera potřebná k pozdějšímu přestřižení vodiče. Svorkou Z je přípravek připojen ke druhému z vodičů. Na počátku je odpor rezistoru A nastaven na nulu, spínač S je rozepnutý a odpor rezistoru B je nastaven na stanovenou hodnotu (viz dále).



Obrázek 6: Schéma sabotážního přípravku s potenciometry.

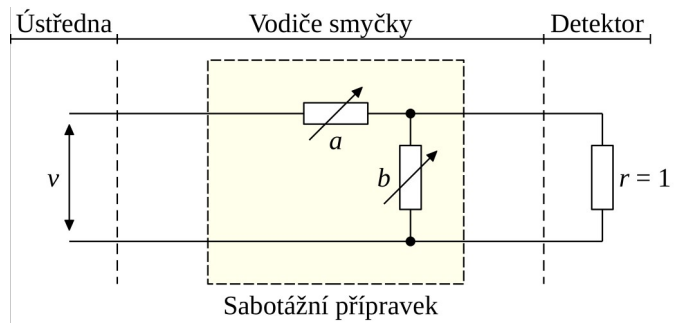
K podrobnějšímu vysvětlení této sabotážní techniky bude použit matematický model. V tomto modelu jsou použity relativní hodnoty odporů, přičemž vztažnou hodnotou je hodnota vyvažovacího odporu R . Potom relativní odpor smyčky $v = V/R$, relativní odpory proměnných rezistorů $a = A/R$, resp. $b = B/R$ a relativní odpor vyvažovacího rezistoru $r = R/R = 1$. Relativní horní hranice tolerančního pásma $m = M/R$ a relativní dolní hranice $n = N/R$.

Dalšími parametry modelu jsou veličiny e , resp. d , které nazveme horní, resp. dolní relativní šířka tolerance $e = m - 1$, resp. $d = 1 - n$. S nimi souvisí parametr $\tau = d + e$, což je relativní celková šířka tolerančního pásma ústředny (viz také obrázek 9). Že jde o relativní hodnoty, lze zjistit podle malého písmena použitého k označení dané veličiny. Proto, pokud nehrozí nedorozumění, tak bude slovo „relativní“ v dalším textu vynecháváno. Sabotáž probíhá po krocích, které jsou indexovány proměnnou i , přičemž okamžik zahájení i -tého kroku je označen proměnou t_i a hodnoty odporů a , b a v v těchto okamžicích jsou značeny a_i , b_i a v_i .

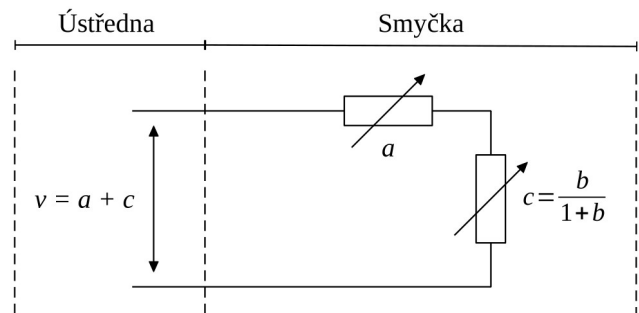
Když je sabotážní přípravek plně zapojen do smyčky, tak vznikne obvod podle obr. 7. V uvedeném obvodu je rezistor a s aktuální hodnotou odporu a_i zapojen v sérii s paralelní kombinací nastavitelného rezistoru b o hodnotě b_i a vyvažovacího rezistoru s hodnotou odporu $r = 1$. Paralelní kombinace odporů b a r je v použitém modelu nahrazována ekvivalentním odporem c s hodnotou:

$$c_i = \frac{r \cdot b_i}{r + b_i} = \frac{b_i}{1 + b_i}, \quad (1)$$

čímž získáme náhradní schéma smyčky podle obrázku 8.



Obrázek 7: Sabotážní přípravek ve smyčce.



Obrázek 8: Náhradní schéma smyčky.

Pro celkový odpor v_i této smyčky platí vztah:

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

Princip sabotáže spočívá v tom, že opakovaným zvýšením hodnoty a , které je následováno snížením hodnoty b (a tedy také hodnoty c), se udržuje výsledný odpor smyčky v v tolerančním pásmu $\langle n, m \rangle$. Hodnota a se tím přibližuje k hodnotě $r = 1$ a hodnota b se přibližuje k nule. Nakonec je dosažen stav, kdy $a = r = 1$ a kdy vyvažovací rezistor r v detektoru je zkratován nulovou hodnotou b . Detektor pak lze od ústředny odpojit bez toho, že by byla signalizována sabotáž.

Na začátku sabotáže je vodič mezi svorkami X a Y nepřerušovaný, odpor rezistoru a je nastaven na nulu (tj. $a_0 = 0$), spínač S je rozepnutý a odpor rezistoru b je nastaven na hodnotu b_0 (podrobněji viz dále). V okamžiku t_0 je sepnut spínač S , čímž je k rezistoru $r = 1$ paralelně připojen rezistor o hodnotě odporu b_0 . Dojde tak ke skokovému snížení hodnoty odporu v smyčky, přičemž se požaduje, aby nedošlo k vyhlášení sabotáže. Musí tedy platit:

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

Ke snížení hodnoty v na dolní hranici n tolerančního pásma při podmínce $a_0 = 0$ musí pro b_0 platit:

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

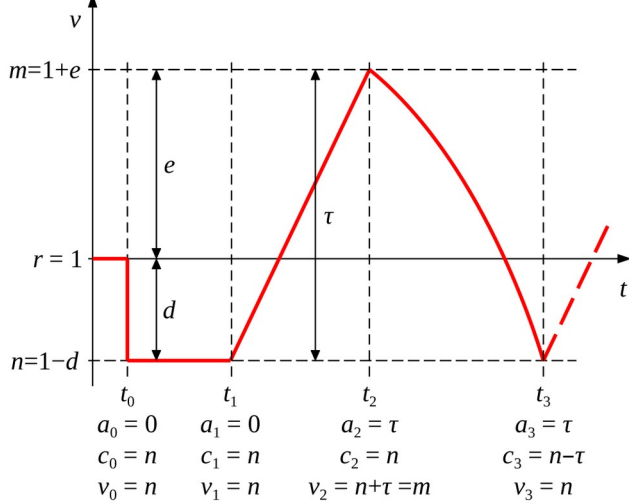
Řešením této rovnice je hodnota

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

Pokud se tedy na začátku sabotáže nastaví rezistor b právě na tuto hodnotu, tak podle vztahu (3) dojde sepnutím spínače

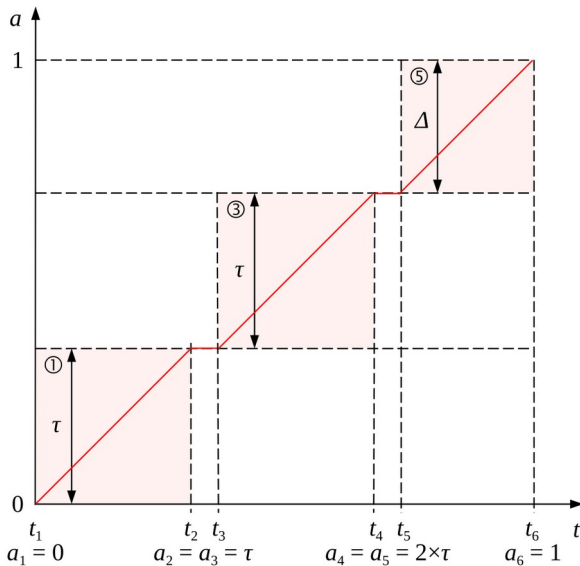
S v čase t_0 k tolerovanému poklesu odporu smyčky na hodnotu $v_0 = 1-d = n$ (viz obrázek 9). A protože $a_0 = 0$, tak tato hodnota je zároveň počáteční hodnotou c_0 odporu paralelní kombinace rezistorů b a r .

V čase t_1 je přestřižen vodič mezi svorkami X a Y, čímž se do smyčky zapojí rezistor a s hodnotou $a_1 = a_0 = 0$. Odpor smyčky v se tím nezmění, tj. $v_1 = v_0$. Následným zvýšením hodnoty odporu proměnného rezistoru a na hodnotu $a_2 = \tau$ se dosáhne toho, že podle (2) bude v čase t_2 odpor smyčky $v_2 = v_1 + a_2 = n + \tau = m$, tj. odpor smyčky bude na tolerovaném maximu m . Poté se začne snižovat hodnota b , čímž zároveň dojde ke snížení hodnoty c . V čase t_3 bude uvedená hodnota snížena o hodnotu τ , takže v tomto okamžiku bude odpor smyčky $v_3 = m - \tau = n$, tj. odpor smyčky nyní bude zpátky na tolerovaném minimu n . Takto se střídavě postupuje dále.



Obrázek 9: Princip sabotáže.

Nyní je možné vysvětlit trajektorii hodnoty v v tolerančním pásmu podrobněji. Jak již bylo zmíněno, účelem přípravku je postupně odpor a zvýšit z hodnoty 0 na hodnotu $r = 1$ a odpor b snížit z hodnoty b_0 na 0. Příklad odpovídajícího průběhu změn odporu rezistoru a v závislosti na čase je na obrázku 10.

Obrázek 10: Průběh změn odporu a .

Hodnota a bude v našem příkladu narůstat ve třech fázích, které jsou označeny symboly ①, ③ a ⑤. Fáze s označením ① proběhne v časovém intervalu t_1 až t_2 a během ní vzroste odpor a z hodnoty $a_1 = 0$ na hodnotu $a_2 = \tau$. V intervalu t_2 až t_3 se pomocí b mění hodnota c , takže v tomto intervalu se hodnota a nemění, tj. $a_2 = a_3$. Pak bude v intervalu t_3 až t_4 následovat fáze ③, během které je odpor a_3 znovu zvýšen o hodnotu τ , tj. na hodnotu $a_4 = 2 \times \tau$. Následuje interval t_4 až t_5 , kdy se mění hodnota c , takže v tomto intervalu bude hodnota a opět beze změny. V intervalu t_5 až t_6 proběhne fáze ⑤, během které odpor a konečně dosáhne cílovou hodnotu $a_6 = 1$. Z obrázku je zřejmé, že nárůst Δ odporu a v této finální fázi je obecně menší než hodnota τ . Pro zbytkový odpor Δ formálně platí, že:

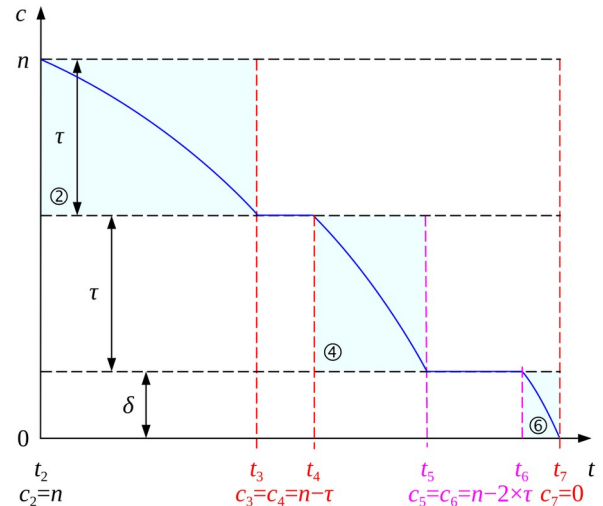
$$\Delta = 1 - K \times \tau, \quad (6)$$

kde K je počet zvýšení odporu a o hodnotu τ . Pro K samozřejmě platí, že:

$$K = \left\lfloor \frac{1}{\tau} \right\rfloor, \quad (7)$$

kde zápis $\lfloor x \rfloor$ vyjadřuje dolní celou část čísla x . V našem případě $K = 2$.

Příklad časového průběhu změn odporu c je na obrázku 11. Jak již bylo zmíněno, u tohoto odporu je cílem snížit jeho hodnotu z hodnoty $n = 1-d$ na hodnotu 0.

Obrázek 11: Průběh změn odporu c .

V našem příkladu hodnota c klesá ve třech fázích, které jsou označeny symboly ②, ④ a ⑥. Fáze ② proběhne v časovém intervalu t_2 až t_3 a během ní klesne odpor c z hodnoty $c_2 = n$ na hodnotu $c_3 = n - \tau$. V intervalu t_3 až t_4 dochází k úpravě hodnoty a , takže v tomto intervalu se hodnota c nemění, tj. $c_3 = c_4$. V intervalu t_4 až t_5 proběhne fáze ④, během které odpor c_4 klesne opět o hodnotu τ , tj. na hodnotu $c_5 = n - 2 \times \tau$. V intervalu t_5 až t_6 je opět upravována hodnota a , takže v daném intervalu je hodnota c beze změny. V intervalu t_6 až t_7 pak proběhne fáze ⑥, během které odpor c konečně dosáhne cílovou hodnotu $c_7 = 0$. Pokles δ odporu c v této finální fázi je obecně menší než hodnota τ . Pro hodnotu zbytkového odporu δ formálně platí, že:

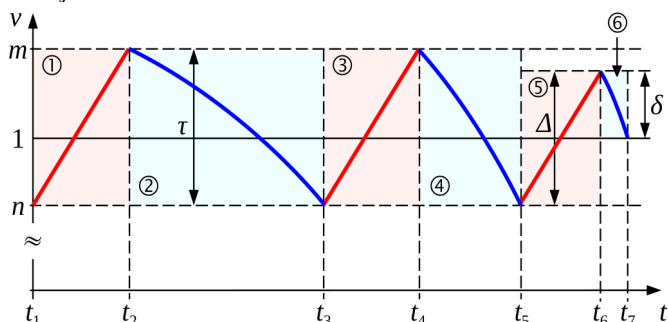
$$\delta = n - L \times \tau, \quad (8)$$

kde L je počet snížení odporu b o hodnotu τ . Pro L samozřejmě platí, že:

$$L = \left\lfloor \frac{n}{\tau} \right\rfloor, \quad (9)$$

kde zápis $[x]$ vyjadřuje dolní celou část čísla x . V našem případě $L = 2$.

Z průběhů na obrázcích 10 a 11 nyní lze pro náš příklad sestavit výslednou trajektorii odporu v smyčce. Uvedená trajektorie je na obrázku 12.



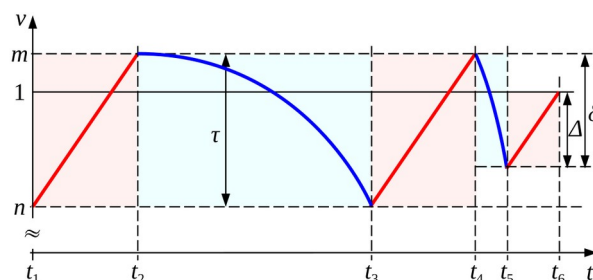
Obrázek 12: Příklad trajektorie odporu smyčky při sabotáži.

Prakticky se jedná o seřazení výše popsaných fází ① až ⑥ do jediného průběhu. Tento průběh začíná v čase t_1 s hodnotami $a_1 = 0$ a $c_1 = n$, takže výsledný odpor smyčky $v_1 = a_1 + c_1 = n$. Ve fázi ① se zvýší odpor a o hodnotu τ , takže v čase t_2 platí, že $a_2 = \tau$ a $c_2 = n$. Potom odpor smyčky $v_2 = n + \tau = m$. Následuje pak fáze ②, během které se hodnota odporu c o hodnotu τ sníží. V čase t_3 tak platí, že $a_3 = \tau$ a $c_3 = n - \tau$ a hodnota $v_3 = n$. Stejně je to i u fází ③ a ④, takže v čase t_5 jsou nakonec hodnoty odporů $a_5 = 2 \times \tau$ a $c_5 = n - 2 \times \tau$ a výsledný odpor smyčky $v_5 = a_5 + c_5 = n$. Ve fázi ⑤ dojde ke zvýšení hodnoty a o zbytkový odpor Δ , takže $a_6 = 2 \times \tau + \Delta = 1$, $c_6 = c_5 = n - 2 \times \tau$ a odpor smyčky $v_6 = a_6 + c_6 = n + \Delta$. Ve fázi ⑥ pak nakonec dojde ke snížení c o zbytkový odpor δ a tak v čase t_7 platí, že $a_7 = 1$ a $c_7 = c_6 - \delta = (n - 2 \times \tau) - \delta = n - (2 \times \tau + \delta) = n - n = 0$. Konečná hodnota odporu smyčky $v_7 = a_7 + c_7 = 1$.

Výše popsaná trajektorie je pouze jedním konkrétním případem. Zcela obecně trajektorie odporu v začíná v okamžiku t_1 na hodnotě n , dále následuje K vzestupů odporu v o hodnotu τ , které jsou proloženy L poklesy o hodnotu τ . Pak následuje vzestup odporu v o hodnotu Δ spolu s poklesem o hodnotu δ . Pořadí finálního vzestupu, resp. poklesu závisí na hodnotách K a L . Pokud $K = L$, tak nejprve proběhne vzestup následovaný finálním poklesem. Příklad této trajektorie je na obrázku 12, kde $K = L = 2$. V případě $K = L + 1$, však nejprve proběhne finální pokles, který je následován finálním vzestupem. Příklad této varianty pro $K = 2$ a $L = 1$ je na obrázku 13.

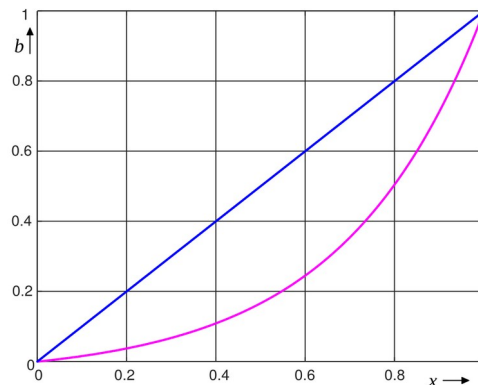
Závěrem lze konstatovat, že popsanou sabotážní technikou útočník střídavě zvyšuje odpor a a následně snižuje hodnotu odporu c , tak aby odpor smyčky udržel v tolerančním pásmu $\langle n, m \rangle$. Ke správnému nastavení hodnot využívá předem vytvořené značky na stupnicích potenciometrů. Uvedeným způsobem se útočník postupně přibližuje s hodnotou a k hodnotě $r = 1$ a s hodnotou c se přibližuje k nule. Nakonec dosáhne stav, kdy $a = r = 1$ a kdy vyvažovací rezistor R v detektoru bude zkratován nulovou hodnotou b . Potom detektor i s jeho vyvažovacím rezistorem může od vedení odstříhnout bez toho, že

by ústředna ohlásila sabotáž. Na přestřižené vodiče u svorek Y a Z útočník připojí falešný rezistor R' o odporu R a opačným postupem se vrátí do počátečního stavu. Nakonec útočník propojí oba konce přestřiženého vodiče mezi svorkami X a Y, sabotážní přípravek odpojí a sabotáž vhodně zamaskuje.



Obrázek 13: Příklad trajektorie odporu v smyčce pro $K \neq L$.

Nyní ještě pár slov k možnosti zkvalitnění sabotážního přípravku s potenciometry. Z obrázku 11 je zřejmé, že výsledný odpor c paralelní kombinace b a r klesá ke konci sabotáže velmi strmě. V této fázi pak malá chyba v nastavení pozice potenciometru B může způsobit vyhlášení sabotáže. K minimalizaci uvedeného rizika je vhodné namísto lineárního použít potenciometr logaritmický. Normalizovaný průběh odporu b lineárního a logaritmického potenciometru je uveden na obrázku 14. Na vodorovné ose grafu jsou uvedeny hodnoty proměnné x , což je aktuální vzdálenost jezdce potenciometru od počátku odporové dráhy v poměru k celkové délce odporové dráhy potenciometru. Modře je znázorněn průběh odporu u lineárního potenciometru a fialově u logaritmického potenciometru.



Obrázek 14: Průběh relativního odporu b u lineárního (modře) a logaritmického (fialově) potenciometru.

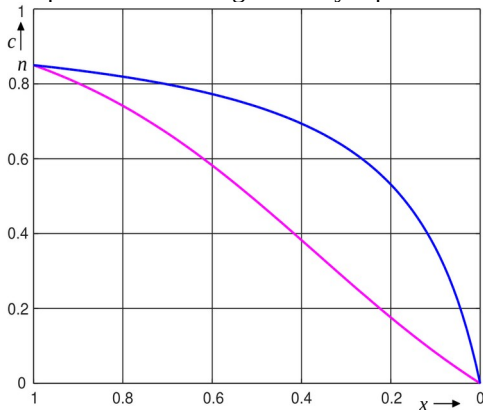
Logaritmické potenciometry se nazývají logaritmické proto, že logaritmus jejich odporu v závislosti na hodnotě x je prakticky přímka. Průběh odporu je tedy dán exponenciální rovnicí $b = w^x$, kde w je maximální hodnota odporu potenciometru. Problémem u této rovnice však je, že pro $x = 0$ vyjde odpor b nenulový, což je v rozporu s fyzikální realitou. Proto se používají různé aproximace, přičemž v článku je použita následující:

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

Uvedená aproximace obsahuje exponenciální člen w^x a zároveň splňuje požadavek, že pro $x = 0$ je $b = 0$ a pro $x = 1$ je b

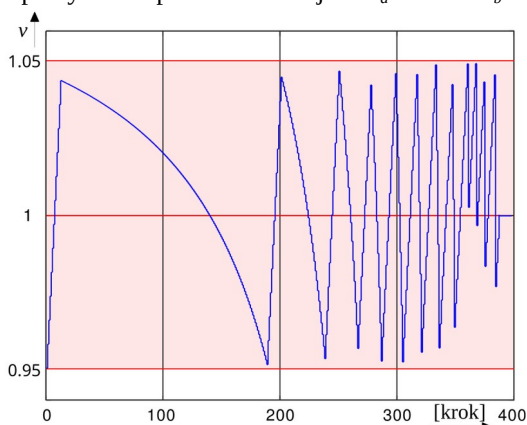
$= w$. Parametr p je relativní odpor potenciometru v polovině jeho dráhy (tj. hodnota b pro $x = 0,5$). Většina výrobců vyrábí potenciometry s hodnotou p v intervalu $(0,15, 0,2)$ (např. [10], s. 85). V dalším je použita hodnota $p = 1/6$, takže $w = 25$.

Závislost odporu paralelní kombinace rezistorů b a r , tj. průběh výsledného relativního odporu c , je pro oba typy potenciometrů uveden na obrázku 15. Modrý průběh platí pro lineární potenciometr a fialový průběh platí pro logaritmický. Průběhy jsou pro pozice jezdce od hodnoty $x = 1$ (to znamená od maximální hodnoty odporu) po $x = 0$ (tj. po nulový odpor). Z obrázku je zřejmé, že fialový průběh má téměř lineární charakter, takže v sabotážním přípravku je u rezistoru B vhodnější použít právě potenciometr s logaritmickým průběhem.



Obrázek 15: Průběh relativního odporu c u lineárního (modře) a logaritmického (fialově) potenciometru v závislosti na relativní pozici jezdce potenciometru.

Další možné zdokonalení sabotážního přípravku s potenciometry spočívá v náhradě mechanických potenciometrů digitálními. Odpor tohoto typu potenciometrů je možné nastavovat elektronicky v k krocích, kde typicky $k = 128$ nebo 256 (např. [11]). Přípravek by pak mohl být řízen jednoduchým procesorem, čímž by bylo možné dosáhnout vyšší přesnosti a zároveň vyšší rychlosti sabotáže. Bylo by také možné sabotovat smyčky u ústředny s extrémně úzkým tolerančním pásmem τ . Na obrázku 16 je uveden možný průběh změn odporu smyčky v pro případ, kdy relativní odpory potenciometrů $a = 1$, $b = 19$, přičemž počty kroků potenciometrů jsou $k_a = 128$ a $k_b = 256$.



Obrázek 16: Trajektorie odporu smyčky u přípravku s digitálními potenciometry.

Ve zmiňovaném příkladu zůstává odpor smyčky v pásmu $v = 1 \pm 0,05$ (červeně zvýrazněno). I kdyby ústředna měla takovouto extrémně úzkou toleranci klidového stavu (tj. $\pm 5 \%$), tak by sabotáž byla úspěšná. K průběhu na obrázku je zapotřebí ještě poznamenat, že relativní odpor v smyčce se na rozdíl například u obrázku 12, či 13 k hraničním hodnotám $m = 1,05$ a $n = 0,95$ jen přibližuje. Je to dáno tím, že odpor digitálních potenciometrů se mění diskrétně a nikoliv spojitě.

4 Závěr

V úvodu článku je řešena problematika smyčkových poplachových systémů. Tento typ systémů je sice postupně nahrazován digitálními poplachovými systémy, avšak stále platí, že smyčkové systémy jsou v praxi široce zastoupeny. Hlavním tématem článku je útok na smyčkové systémy tzv. sabotáží smyček. Ve veřejně dostupné literatuře jsou široce publikovány pouze sabotáže jednoduchých smyček. Prakticky použitelné sabotáže vyvážených smyček, které jsou v praxi zcela nejrozšířenější, publikovány nejsou. Majitelé smyčkových poplachových systémů tak mohou vcelku oprávněně předpokládat, že u systémů s vyváženými smyčkami sabotáže prakticky nehrozí.

V článku jsou popsány dvě techniky sabotáže vyvážených smyček. První technika je založena na skokové náhradě vyvažovacího rezistoru o odporu R falešným rezistorem o téměř odporu (viz obrázek 5). K úspěšnému přepnutí rezistorů postačil obyčejný mechanický přepínač. Nevýhodou přepínací techniky je krátkodobé přerušení smyčky, které ústředny s vyšší úrovní bezpečnosti nemusí tolerovat.

Z tohoto pohledu je druhá technika zcela obecná. Ústředny totiž musí respektovat skutečnost, že z praktických důvodů se odpor smyčky může pohybovat v rozmezí od určité minimální hranice N po maximální hranici M . V rámci sabotáže se do smyčky vloží sériově-paralelní kombinace potenciometrů (viz obrázek 6). Na počátku je odpor sériového potenciometru nulový a odpor paralelního potenciometru dostatečný na to, aby výsledný odpor smyčky neklesl pod minimální hranici N . Zvyšováním odporu sériového potenciometru, které je střídáno snižováním odporu paralelního potenciometru, se výsledný odpor smyčky udržuje v hranicích N a M . Konečným cílem je stav, kdy paralelní potenciometr zkratuje vyvažovací rezistor detektoru a sériový potenciometr převezme úlohu vyvažovacího rezistoru smyčky.

K realizaci obou výše popsaných sabotáží musí mít útočník přístup k vodičům smyčky. Vodiče jsou nejčastěji vedeny buď pod omítkou nebo v lištách. Pokud jsou vodiče vedeny pod omítkou, tak je sabotáž složitější, ale stále možná. Vodiče vedené v lištách jsou dostupnější mnohem snáze a tak riziko sabotáže smyčky bude u takovýchto systémů mnohem vyšší.

Z popisu obou sabotážních technik je zřejmé, že příslušné přípravky jsou technicky jednoduché a laciné. Zhotovit a použít je zvládne i amatér. Majitelé poplachových systémů by se proto měli o této hrozbě dozvědět, aby mohli její nebezpečí pro svůj systém vyhodnotit. Reagovat na zmíněnou hrozbu je však bohužel obtížné. Zejména druhá ze sabotážních technik je prakticky nedetekovatelná, protože u ní nedochází k přerušení smyčky. Navíc může fungovat i u ústředny s extrémně úzkým tolerančním pásmem (viz obrázek 16). Možné ochrany

spočívají ve ztížení přístupu k vodičům smyček a v monitorování tras smyček například pomocí detektorů otřesů, obhlídkami a kamerovými systémy. Tyto ochrany jsou však jen částečné. Principiálním řešením je migrace na kvalitní digitální zabezpečovací systém. Pokud je kvalitně kryptograficky zabezpečen, tak je sabotáž komunikace ústředny s detektorem prakticky vyloučena.

Literatura

- [1] Pope A. R.: Improvement in electro-magnetic alarms. Patent US9802A, United States Patent Office, Washington 1853. Dostupné na: <https://patents.google.com/patent/US9802?q=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. Dostupné na: <https://bit.ly/3Km47nr>
- [5] -: ATS control panel. Installation guide. GE Security, Boston 2007. Dostupné na: <https://bit.ly/40KYXqI>
- [6] -: JA-116H BUS expander. Jablotron, Jablonec nad Nisou. Dostupné na: <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. Technický list. Piher Sensors & Controls, Tudela. Dostupné na: <https://bit.ly/40udRBG>
- [11] -: MCP41HVX1. Technický list. Microchip Technology, Chandler 2013. Dostupné na: <https://bit.ly/3nLk5ih>