Způsoby zabezpečení drátových ústředen EZS proti sabotáži

Security methods of wired central ESS against sabotage

Adam Hanáček

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Adam HANÁČEK**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Způsoby zabezpečení drátových ústředen EZS proti sabotáži.**

Zásady pro vypracování:

1. **Prostudujte doporučenou literaturu a zpracujte literární rešerši na dané téma.**
2. **Zaměřte se na drátové ústředny typu NO a NC.**
3. **Rozeberte možnosti zapojení smyček včetně způsobu ochrany proti sabotáži, popište výhody a nevýhody jednotlivých zapojení.**
4. **Vypracujte návrh, jak lze ochranu proti sabotáži obejít.**
5. **Účinnost návrhu odzkoušejte na libovolné ústředně v laboratoři UTB.**

Rozsah práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Křeček, S.: Příručka zabezpečovací techniky, Blatenská tiskárna s.r.o, Blatná,**
2. **ISBN 80-902938-2-4**
3. **KINDL, J.: Projektování bezpečnostních systémů, UTB Zlín, 2007**
4. **Černý, J., Ivanka J a kol.:, Systemizace bezpečnostního průmyslu I, UTB Zlín, 2006**
5. **ČSN EN 50131 Poplachové systémy - Elektrické zabezpečovací systémy**
6. **UHLÁŘ, J.: Technická ochrana objektů II. Díl - Elektrické zabezpečovací systémy, Praha, Policejní akademie ČR, 2001. ISBN 80-7251-076-2.**

Vedoucí bakalářské práce: **Ing. Milan Navrátil, Ph.D.**
Ústav elektroniky a měření

Datum zadání bakalářské práce: **19. února 2010**

Termín odevzdání bakalářské práce: **19. května 2010**

Ve Zlíně dne 19. února 2010

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Teoretická část práce popisuje změny v normě ČSN EN 50131-1, která se zabývá poplachovými systémy. Dále práce obsahuje popis jednotlivých částí ústředny, přičemž hlavní důraz je kladen na ochranu analogových ústředen poplachových zabezpečovacích systémů (PZS) před sabotáží včetně požadavků aktuální normy ČSN EN 50131-1/A1. V praktické části je popsán vlastní návrh pro testování bezpečnosti drátových analogových ústředen PZS včetně praktické realizace na ústředně Spectra.

Klíčová slova: PZS, ústředna, poplach, sabotáž, norma.

ABSTRACT

The theoretical part of the work describes changes of the norm ČSN EN 50131-1, which deals with alarm systems. The work also contains description of the individual parts of security centrals, whereas the main accent lays in protecting of analog wired centrals against sabotage including the requirements of actual norm ČSN EN 50131/A1.

In the practical part, own suggestions for testing of security on wired analog centrals IAS including practical realization of the central Spectra are given.

Keywords: IAS, central, alarm, sabotage, norm.

Rád bych poděkoval vedoucímu mé bakalářské práce Ing. Milanu Navrátilovi, Ph.D. za cenné připomínky, rady, věnovaný čas a trvalý zájem.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Se zvyšující se životní úrovní se zvyšuje i ochota lidí investovat do ochrany svého majetku. Existuje mnoho firem, které se zabývají ochranou majetku, a existují různé způsoby, kterými lze majetek chránit. V mé bakalářské práci popisuji drátové ústředny elektronických zabezpečovacích systémů (EZS).

Elektronický zabezpečovací systém nezastaví narušitele objektu, ale pouze pošle informaci o narušení objektu a spustí poplachovou signalizaci (optickou nebo akustickou). Informace se posílá zpravidla na pult centralizované ochrany nebo mobilní telefon. Levnější je poslat informaci na mobilní telefon, ovšem je důležité uvědomit si, že při narušení objektu hraje roli každá vteřina a je potřeba objekt co nejrychleji zkontrolovat. Málokdo má možnost rychle zajistit kontrolu objektu. Navíc je potřeba zvážit i příslušná rizika související s nebezpečností pachatele. Proto existují pulty centralizované ochrany, což jsou specializovaná pracoviště, která zajišťují kontrolu objektu do určitého času a která mají specializované pracovníky, kteří jsou proškoleni o možných nebezpečných situacích. Další výhodou elektronických zabezpečovacích systémů je ochrana života a zdraví. Současné ústředny lze naprogramovat i tak, aby byl objekt hlídán jen pomocí některých zařízení ze zabezpečovacího systému. Tím lze například na noc střežit jen určité prostory, kde se nepohybujeme, nebo plášť objektu (okna, dveře). V případě vniknutí se spustí poplachová signalizace a může se zabránit nebezpečnému střetnutí majitele objektu s narušitelem.

Bakalářská práce popisuje úlohu a jednotlivé části drátových ústředen elektronických zabezpečovacích systémů. Hlavní důraz je kladen nejen na požadavky současných platných norem ČSN EN 50131-1, ale i princip ochrany analogových drátových ústředen EZS proti sabotáži. Dále práce obsahuje vlastní návrh pro testování bezpečnosti zmíněných ústředen včetně praktické realizace a ze zjištěných poznatků jsou popsány možnosti řešení vzniklého problému. Vzhledem k neustálé snaze zlodějů proniknout do bezpečnostního systému s cílem ukrást cizí majetek, je velmi důležité sledovat aktuální normy, které se týkají poplachových zabezpečovacích systémů, a testovat používané poplachové systémy před nebezpečným překonáním. V případě zjištění nedostatku je nezbytně nutné realizovat takové opatření, které minimalizuje riziko překonání elektronických zabezpečovacích systémů.

I. TEORETICKÁ ČÁST

1 ELEKTRONICKÉ ZABEZPEČOVACÍ SYSTÉMY

1.1 Změna názvu EZS podle normy ČSN EN 50131-1 ed.2

Norma na rozdíl od předchozího vydání rozlišuje poplachové systémy pro detekci vniknutí a poplachové systémy pro detekci přepadení. V souvislosti s tím jsou některé body této normy formulovány odděleně pro tyto dva druhy zabezpečení. V originále této normy se kromě jediné zkratky, IAS (Intruder Alarm System-poplachový systém pro detekci vniknutí), použité v předchozím vydání normy, objevuje zkratka I&HAS (Intruder and Hold-up Alarm Systém-poplachový systém pro detekci vniknutí a přepadení). Na několika místech normy jsou použity zkratky HAS (Hold-up Alarm Systém-poplachový systém pro detekci přepadení) tam, kde systém postrádá funkci detekce vniknutí, a IAS tam, kde systém postrádá funkci detekce přepadení. Proto jsou nyní v českém překladu normy místo dosud používané zkratky EZS používány zkratky z originálu - I&HAS „poplachové zabezpečovací a tísňové systémy“, IAS pro „poplachové zabezpečovací systémy“ a pro HAS „poplachové tísňové systémy“. V českých textech lze uvedené zkratky z originálu nahradit následujícím způsobem: I&HAS=PZTS, IAS=PZS, HAS=PTS. [1]

1.2 Rozdíl mezi EZS a I&HAS

Změna původní normy ČSN EN 50131, která se zabývala EZS, spočívá ve sloučení s normou ČSN EN 50135 (tísňové systémy). Původní zkratka EZS byla nahrazena IAS a sloučena s HAS. Vznikl tedy I&HAS. Pro IAS (intruder alarm system) se také používá zkratka PZS (poplachový zabezpečovací systém). V bakalářské práci se dále bude používat zkratka PZS.

1.2.1 Elektronický zabezpečovací systém (EZS)

Poplachový systém pro detekci a indikaci přítomnosti, vstupu nebo pokusu o vstup narušitele do střeženého objektu. [2]

1.2.2 Poplachový zabezpečovací systém (intruder alarm system=IAS)

Poplachový systém sloužící k detekování a indikaci přítomnosti, vniknutí nebo pokusu o vniknutí vetřelce do střeženého prostoru.

1.2.3 Tísňový poplachový systém (hold-up alarm system=HAS)

Poplachový systém poskytující uživateli možnost úmyslného vyvolání poplachového stavu. [1]

1.3 Poplachové zabezpečovací systémy

Poplachový zabezpečovací systém je soubor zařízení, jejichž hlavním úkolem je střežit předem definovaný prostor.

Při vniknutí neoprávněné osoby systém signalizuje narušení prostoru (akusticky nebo opticky) a vyšle informaci o vzniklé situaci na mobilní telefon nebo pult centralizované ochrany, což je specializované pracoviště, ze kterého vyjedou bezpečnostní jednotky, aby zkontrolovaly hlídaný objekt.

V praxi je posílání informace na mobilní telefon velmi rozšířené, ovšem nelze jej doporučit, protože málokdo je schopen zkontrolovat svůj majetek dřív, než pachatel odejde. V druhé řadě je třeba si uvědomit, že pachatel může být ozbrojený a nebezpečný. Z toho důvodu se doporučuje zvolit raději pult centralizované ochrany, kde jsou proškolení pracovníci, kteří přesně vědí, jak se mají zachovat.

Poplachová zabezpečovací signalizace se skládá z detektorů, prostředků poplachové signalizace, poplachové přenosové cesty, zdrojové části, ovládacího zařízení a ústředny.

1.3.1 Detektory

Detektory jsou zařízení, která reagují na fyzikální změny, které souvisí s narušením hlídaného objektu nebo prostoru. Mezi nejpoužívanější detektory patří ultrazvukové detektory, pasivní infračervený detektor, pasivní bezkontaktní detektor rozbití skla, mikrovlnné detektory, otřesové detektory a infrazávory.

1.3.2 Prostředky poplachové signalizace

Jako poplachová signalizace se používá optická nebo akustická indikace narušení objektu. Lze ji také rozdělit jako vnitřní a vnější.

1.3.3 Poplachová přenosová cesta

K přenosu informace mezi ústřednou a pultem centralizované ochrany se používají poplachové přenosové cesty, které lze rozdělit na přenos pomocí telefonní linky, linky GSM, radiové sítě, vyhrazené přenosové cesty a přenos přes internet. Pro zvýšení bezpečnosti se používají dvě přenosové cesty, které jsou navzájem nezávislé.

1.3.4 Zdrojová část

Slouží pro napájení celého systému. Každý elektronický zabezpečovací systém musí mít také záložní baterii pro případ výpadku elektrické energie.

1.3.5 Ovládací zařízení

Ovládací zařízení slouží k ovládání celého systému. Patří zde blokovací zámky (systém se automaticky zastřeží uzamčením zámku), klávesnice, bezdrátová klíčenka nebo karta.

1.3.6 Ústředna

Základní úloha ústředny:

- Přijímá a vyhodnocuje výstupní signály od detektorů
- Signalizuje a vysílá informace o svých stavech
- Napájí detektory a další prvky PZS elektrickou energii
- Zajišťuje diagnostiku stavu PZS
- Ovládá signalizační, přenosové a zapisovací zařízení
- Umožňuje ovládání PZS pomocí ovládacích prvků

Mezi signalizační zařízení patří venkovní sirény, vnitřní sirény a blikače.

Přenosové zařízení umožňuje samočinné předávání výstupních informací do určeného místa po lince jednotné telekomunikační sítě nebo po samostatném vedení nebo po síťovém vedení nebo bezdrátově.

Zapisovací zařízení PZS je zařízení, které umožňuje automatické provedení písemného zápisu výstupních informací ústředny s doplněním identifikačních a časových údajů. [2]

2 DĚLENÍ DRÁTOVÝCH ÚSTŘEDEN PZS PODLE ZPŮSOBU PŘIPOJOVÁNÍ SMYČEK

2.1 Ústředny analogové

U analogových ústředen je každá poplachová smyčka připojena na samostatný vyhodnocovací obvod ústředny. Smyčkou rozumíme skupinu detektorů, které jsou propojeny společným vedením na vstup ústředny. Smyčka je zakončena odporem, který bývá umístněn na konec vedení v posledním detektoru. Detektory se zde připojují sériově nebo paralelně podle způsobu naprogramování ústředny a typu použitých detektorů. Princip analogových ústředen spočívá v měření hodnoty odporu každé smyčky a při změně o více než přibližně 30 % vyhlásí ústředna poplach. Zmíněná tolerance je odlišná a závisí na použité ústředně. Analogové ústředny jsou velmi často používané z důvodu nízké ceny jednotlivých detektorů.

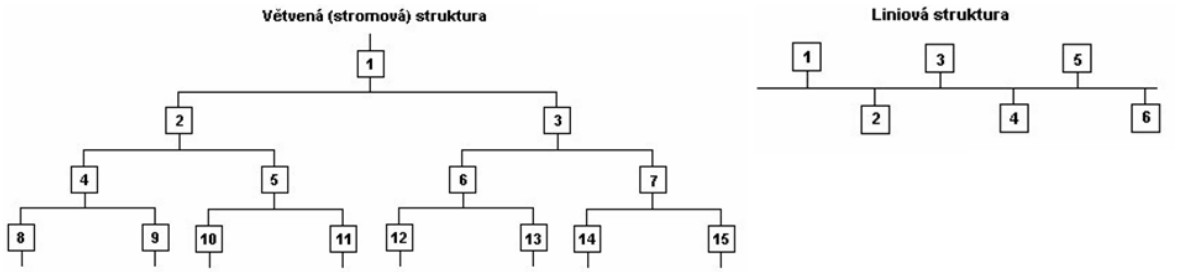
Každý výrobce má v instalačním manuálu zpravidla uveden maximální počet detektorů na smyčce. Nejčastěji se udává maximálně 5 detektorů na jednu smyčku. Podrobné zapojení smyček u analogových ústředen bude popsáno v kapitole 4.

2.2 Ústředny sběrnicové

Ústředny sběrnicové využívají digitální adresné komunikace po datovém vedení (sběrnici-BUS) mezi detektory a ústřednou.

Ústředna je s každým detektorem propojena pomocí čtyř vodičů do příslušných svorek (RED, BLK, GRN, YEL). Svorky RED a BLK slouží pro napájení a GRN a YEL pro komunikaci. Každý detektor musí být vybaven komunikačním modulem. Ústředna periodicky aktivuje adresy jednotlivých detektorů a přijímá příslušné odezvy. Hlavní ochrana proti sabotáži je realizována digitální adresnou komunikací, ve které má každý detektor svou jedinečnou adresu, čímž je zajištěna detekce záměny detektoru. Díky jedinečné adrese je dále možné přesně lokalizovat místo, kde došlo k narušení objektu. Sběrnicové ústředny vynikají vysokou odolností proti překonání. Používají se pro rozsáhlé objekty s možností připojení zpravidla 127 modulů. Délka vedení závisí na úbytku napětí, které nesmí klesnout pod 11 V. [3]

Jednotlivé detektory se připojují paralelně na sběrnici zpravidla pomocí dvou struktur, které jsou vyznačeny na obr. 1 (stromová a liniová).

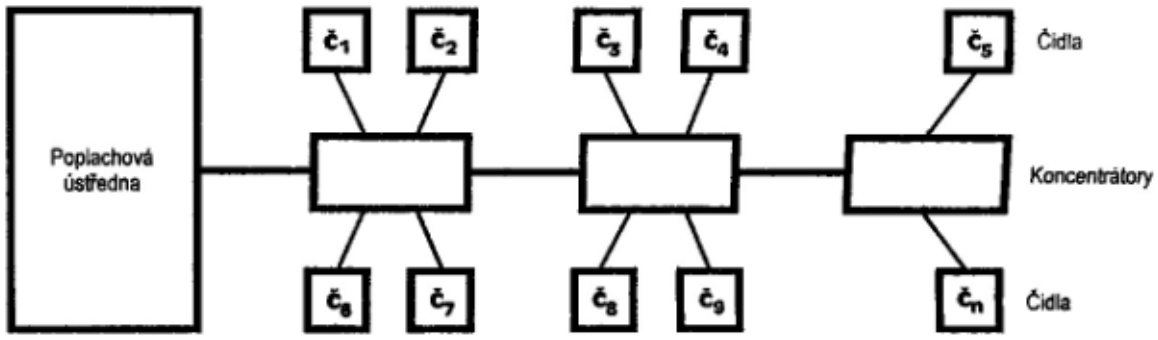


Obrázek 1: Stromová a liniová struktura [4]

2.3 Ústředny koncentrátorové - smíšené

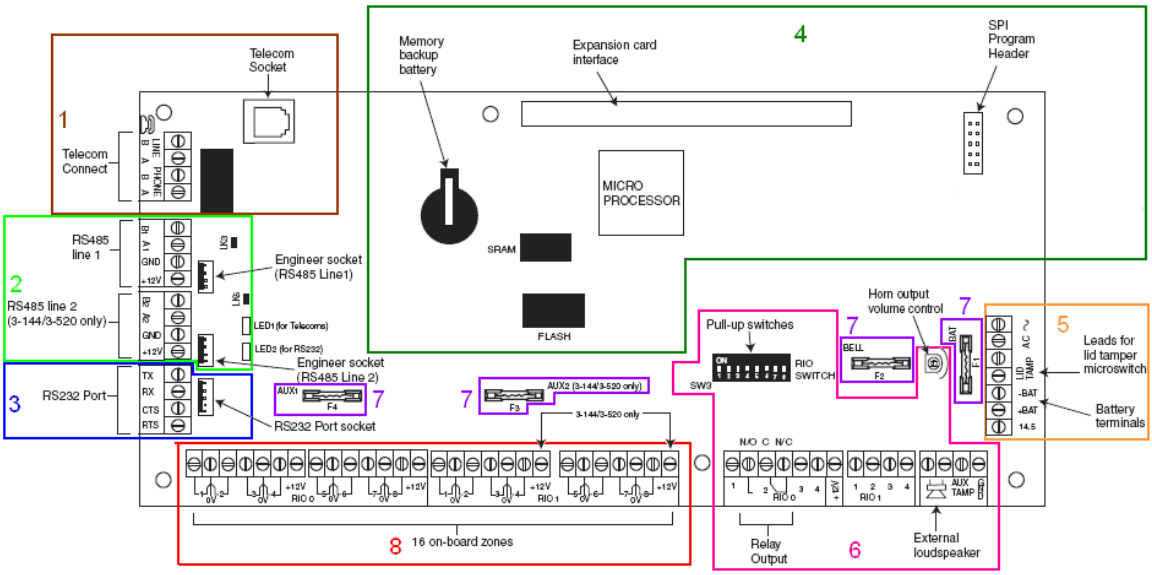
Jedná se o kombinaci sběrnicové a analogové ústředny. Každá ústředna zde má určitý počet linek (sběrnic). Pomocí linek jsou k vlastní ústředně připojeny koncentrátory, které slouží jako analogové několikasmyčkové podústředny. Komunikace mezi ústřednou a koncentrátory probíhá pomocí datové sběrnice, podobně jako u ústředen s přímou adresací detektorů. Detektory jsou na koncentrátory připojeny „klasicky“ pomocí smyček jako u analogových ústředen. [3]

Kromě koncentrátorů (nazývané také jako RIO) se na sběrnici připojuje také klávesnice a komunikační moduly pro připojení tiskárny a počítače. Koncentrátor zpravidla obsahuje 8 adresovatelných smyček (na každou z nich je možné připojit až 10 detektorů) a čtyři programovatelné výstupy. Délka komunikační linky je maximálně 1 km. Příklad propojení zabezpečovacího systému s ústřednou koncentrátorovou je znázorněn na obr. 2.



Obrázek 2. Příklad propojení zabezpečovacího systému s ústřednou koncentrátorovou [3]

3 ZÁKLADNÍ DESKA ÚSTŘEDNY GALAXY G3



Obrázek 3. Základní deska ústředny GALAXY G3 [5]

3.1 Popis jednotlivých částí ústředny Galaxy G3

3.1.1 Telefonní komunikátor a možnosti přenosu zpráv na PCO

Část označená číslem 1 na obr. 3 obsahuje telefonní komunikátor, který lze využít pro komunikaci s PCO. Hlavní výhoda telefonní linky spočívá v tom, že k provozu zpravidla stačí pouze naprogramovat ústřednu. Nevýhodou je pomalý přenos, nutnost telefonní linky v objektu a menší bezpečnost (možnost přerušení vedení). Finanční náklady jsou navýšeny v závislosti na počtu hovorů na PCO. Další možností komunikace ústředny s PCO je pomocí GSM modulu, který má vyšší rychlost a nepotřebuje ke svému fungování telefonní linku. Mezi zápory patří vyšší finanční náklady spojené s instalací GSM modulu, spolehlivost je závislá na momentálním zatížení sítě a navyšují se finanční poplatky za SMS zprávy. Poslední možností je bezdrátové spojení. Jedná se o nejbezpečnější přenos, který funguje v reálném čase, bez zpoždění a není zde potřeba telefonní linky. Finanční náklady spojené s pořízením vysílače jsou vyšší. Pro zajištění největší bezpečnosti se používají dvě přenosové cesty, které jsou navzájem nezávislé.

3.1.2 Datová sběrnice RS 485

Sběrnice RS 485 je na základní desce ústředny označena číslem 2.

Pomocí sběrnice RS 485 lze k ústředně připojit klávesnici, komunikační port RS 232, telefonní komunikátor, systémovou čtečku jako jednu z možností zapnutí a vypnutí systému a koncentrátor G8 RIO pro zvýšení počtu zón a výstupů. Přítomnost všech zařízení, která jsou připojena na sběrnici RS 485, si ústředna neustále kontroluje a v případě selhání zařízení dojde k vyhlášení poplachu. Moduly jsou zde připojeny paralelně a zakončeny zakončovacím odporem. Ústředna Galaxy G3 má dvě linky RS 485. Linku 1 zprovozníme odstraněním konektoru LK3 a linku 2 odstraněním konektoru LK5. Engineer socket slouží pro rychlé připojení servisní klávesnice nebo přídavného modulu.

3.1.3 Komunikátor RS 232

Pod komunikační sběrnicí RS 485 je číslem 3 označen komunikátor RS 232, pomocí kterého lze k ústředně připojit tiskárnu nebo PC.

3.1.4 Paměť se záložní baterií, mikroprocesor, sběrnice pro rozšíření systému a SPI klíč

Jedná se o část na základní desce Galaxy G3, která je vyznačena číslem 4 na obr. 3.

Paměť se záložní baterií slouží pro zachování systémové konfigurace a programovacích detailů. Sběrnice pro rozšíření systému je připravena pro budoucí vývoj systému. Je zde možnost připojit GSM komunikátor, TCP/IP komunikátor nebo RS 485 linky.

Účel SPI klíče spočívá v přepisu a kopírování konfigurace ústředny.

3.1.5 Zdrojová část

Zdrojová část je označena číslem 5 na obr. 3. Pomocí svorek AC lze připojit k ústředně zdroj, který napájí ústřednu elektrickou energii. Úlohou konektoru lid tamper (konektor krytu) je zjištění nedovoleného otevření ústředny. Poslední nezmíněná věc ve zdrojové části jsou konektory BAT, do kterých se připojuje náhradní baterie.

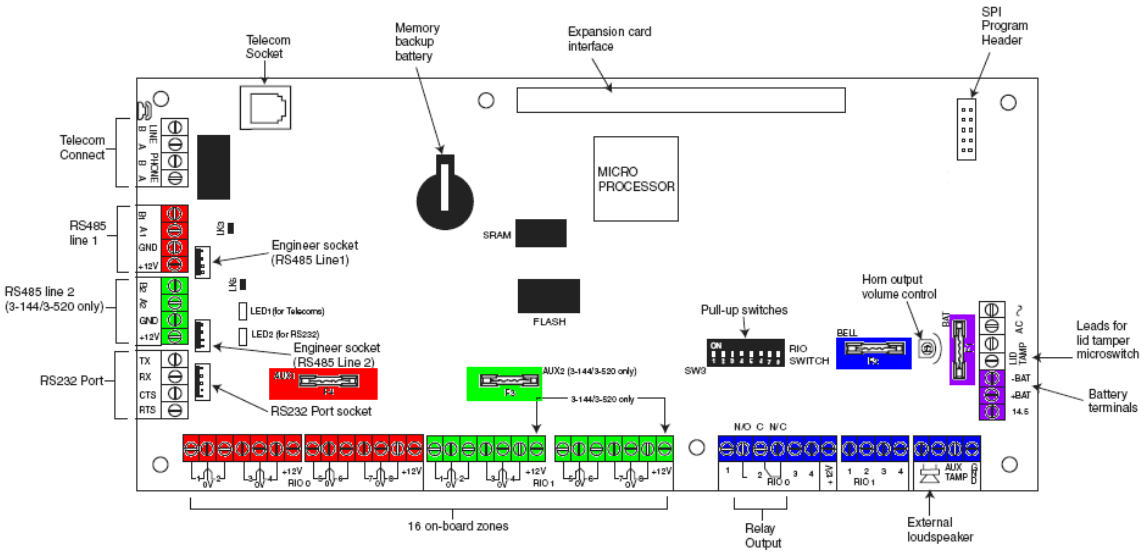
3.1.6 Programovatelné výstupy

Číslem 6 je označena další část, ve které se nachází programovatelné výstupy, jejichž hlavní úlohou je spuštění elektronického zařízení, které signalizuje poplach ústředny (optická nebo akustická indikace).

Galaxy G3 má 7 tranzistorových výstupů (označených jako RIO0 a RIO1) a jeden reléový. Jednotlivé tranzistorové výstupy lze pomocí prvních sedmi přepínačů na SW3 zapnout jako zapojení s otevřeným kolektorem nebo společným emitorem. Poslední přepínač určuje adresu na RIO1. Reléový výstup může být zapojen jako spínací nebo rozpínací podle způsobu zapojeni. Napájení detektorů je prováděno pomocí svorek AUX.

3.1.7 Pojistky

Na základní desce ústředny jsou pojistky označeny číslem 7. Účel spočívá v ochraně před vysokým proudem. Na obr. 4 je barevně rozlišeno, jakou pojistkou jsou chráněny jednotlivé části.



Obrázek 4. Pojistky ústředny GALAXY G3 [5]

3.1.8 Zóny ústředny

Poslední označenou částí s číslem 8 jsou zóny, díky kterým ústředna vyhodnotí jednotlivé stavy detektorů. Napájení detektorů je realizováno pomocí svorek AUX napětím 12 V. Ke každému detektoru tedy vedou dva vodiče pro napájení a dva vodiče pro vyhodnocení stavu detektoru.

4 MOŽNOSTI ZAPOJENÍ SMYČEK V ZÓNĚ U ANALOGOVÝCH DRÁTOVÝCH ÚSTŘEDEN A ZPŮSOBY OCHRANY PŘED SABOTÁŽÍ

Ke každé zóně na ústředně lze připojit jeden nebo více detektorů. Funkce spočívá v neustálém měření odporu ve smyčkách. Při vniknutí nepovolané osoby do objektu detektor změní odpor ve smyčce a ústředna vyhlásí poplach díky spuštění signalizačního zařízení a vyslání informace o poplachu na PCO nebo mobilní telefon. Zapojení detektoru k zóně se rozlišuje na NO (normally opened) a NC (normally closed).

4.1 Požadavky na vedení

Vedení PZS je provedeno pomocí měděných vodičů o průřezu 0,22 mm^2 nebo průměru 0,5 mm. Pro napájení lze použít i silnější vodič, ale to závisí pouze na montážní firmě. V praxi se pro napájení používá zpravidla červená a bílá barva nebo červená a černá barva. Ostatní barvy se používají pro připojení jednotlivých zón.

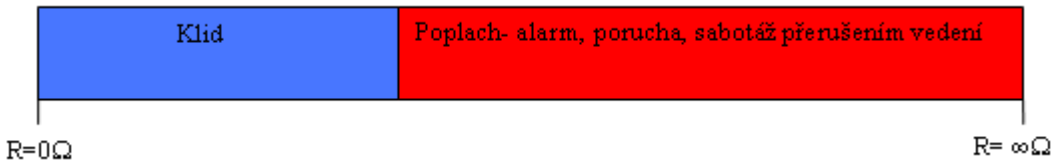
4.2 Možnosti zapojení smyček typu NC (normally closed)

Zapojení typu NC se vyznačuje tím, že kontakty v detektoru jsou v klidovém stavu sepnuty. Při narušení objektu detektor rozepne kontakt a vznikne poplach. Jedná se tedy o rozpínací kontakt.

4.2.1 NC (normally closed)

Při použití typu NC (normally closed) jsou na smyčku připojeny pouze kontakty alarm a jednotlivé detektory se připojují sériově. Na jednu smyčku se doporučuje připojit maximálně 5 detektorů. Když jsou kontakty detektorů sepnuty, je odpor smyčky v zóně velmi malý a ústředna je ve stavu „klid“. Jestliže některý detektor zaznamená narušení hlídané oblasti, rozepne kontakt a odpor smyčky bude velmi velký. Zmíněnou změnu vyhodnotí ústředna jako stav „poplach“. Zapojení má tedy jen stav „klid“ a „poplach“.

Situace je znázorněna na obr. 5.

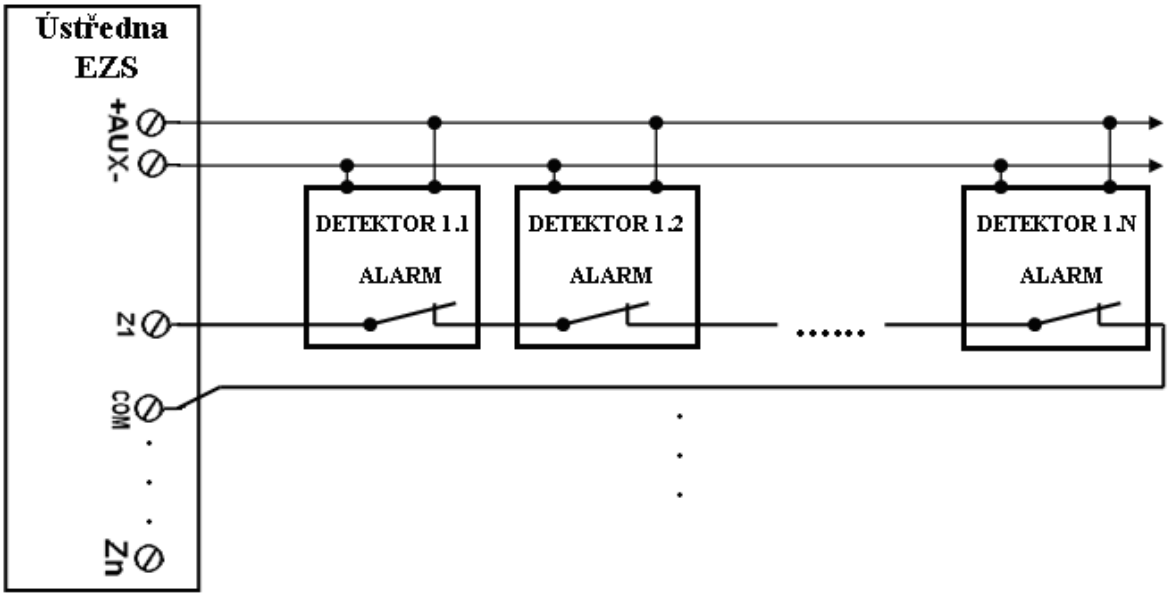


Obrázek 5. Vyhodnocení stavu zóny v závislosti na hodnotě

odporu smyčky typu NC

Mezi nevýhody zapojení patří nemožnost detekce sabotáže pomocí zkratování vedení, nemožnost rozeznání vyhlášení poplachu od přerušení vedení, chybějící kontakt tamper a antimasking. Tamper slouží pro zjištění neoprávněného otevření krytu detektoru a antimasking pro detekci zakrytí detektoru. Zapojení je znázorněno na obr. 6.

Hlavně kvůli možnosti sabotáže pomocí zkratování vedení se uvedené zapojení nesmí používat.



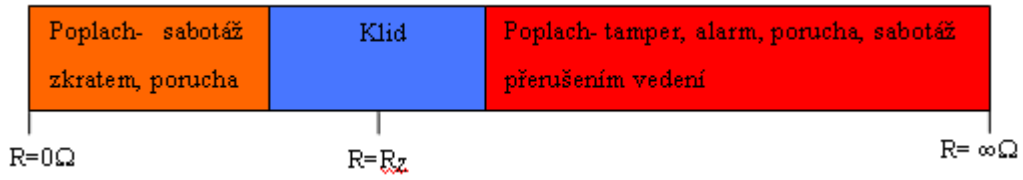
Obrázek 6. Schéma zapojení smyčky typu NC (normally closed)

Svorky AUX slouží pro napájení detektorů a smyčka vyvedená z kontaktu Z1 do COM je vyhodnocovací smyčka.

4.2.2 NC jednoduše vyvážená

V zapojení typu NC jednoduše vyvážená má smyčka navíc zakončovací odpor (na konci vedení v posledním detektoru) a kontakt tamper. Zakončovací odpor zjistí sabotáž na vedení pomocí zkratování a přerušení vedení. Další výhoda je ve zjištění nedovolené

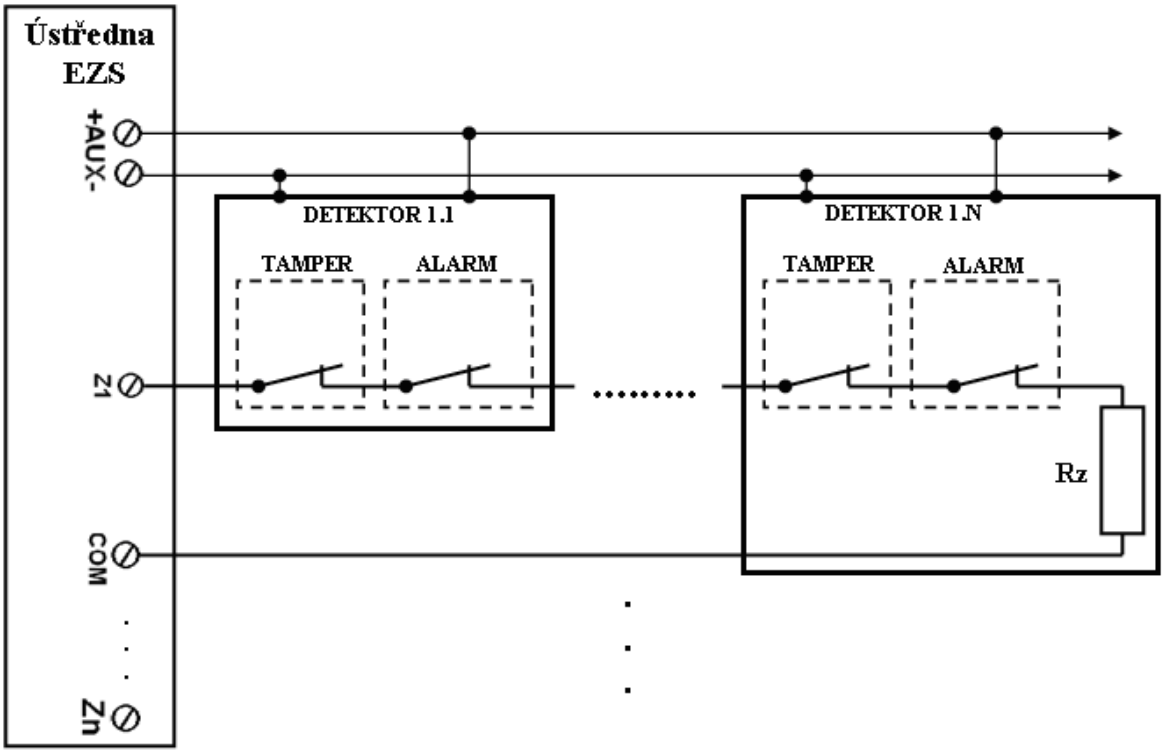
manipulaci s krytem detektoru pomocí kontaktu tamper. Ústředna má tři stavy. Při R=0 Ω je vyhlášen poplach z důvodu zkratování vedení. Když je odpor smyčky přibližně roven Rz (zakončovacímu odporu), ústředna je ve stavu „klid“. Jestliže se rozpojí kontakt tamper nebo alarm, ústředna vyhlásí poplach. Situaci znázorňuje obr. 7.



Obrázek 7. Vyhodnocení stavu zóny v závislosti na hodnotě odporu

smyčky typu NC - jednoduše vyvážená

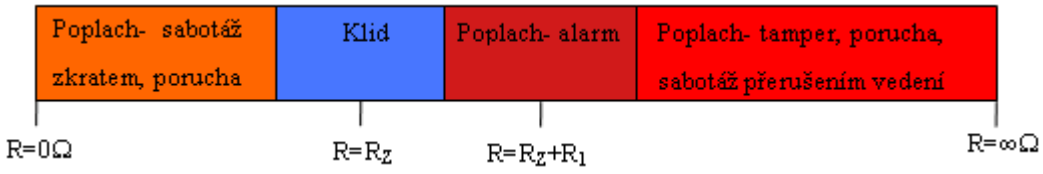
Nevýhodou zapojení je nemožnost rozlišit vyhlášení poplachu pomocí kontaktu tamper od kontaktu alarm a nemožnost detekce zakrytí detektoru. Hodnotu zakončovacího odporu udává výrobce a zpravidla se používá 1 KΩ nebo 2,2 KΩ. U nových ústředen hodnota zakončovacího odporu není pevná, ale lze ji nastavit pomocí programování ústředny. Doporučený maximální počet detektorů na smyčce je zpravidla podle výrobce 5. Zapojení typu NC jednoduše vyvážená je znázorněno na obr. 8.



Obrázek 8. Schéma zapojení smyčky typu NC - jednoduše vyvážená

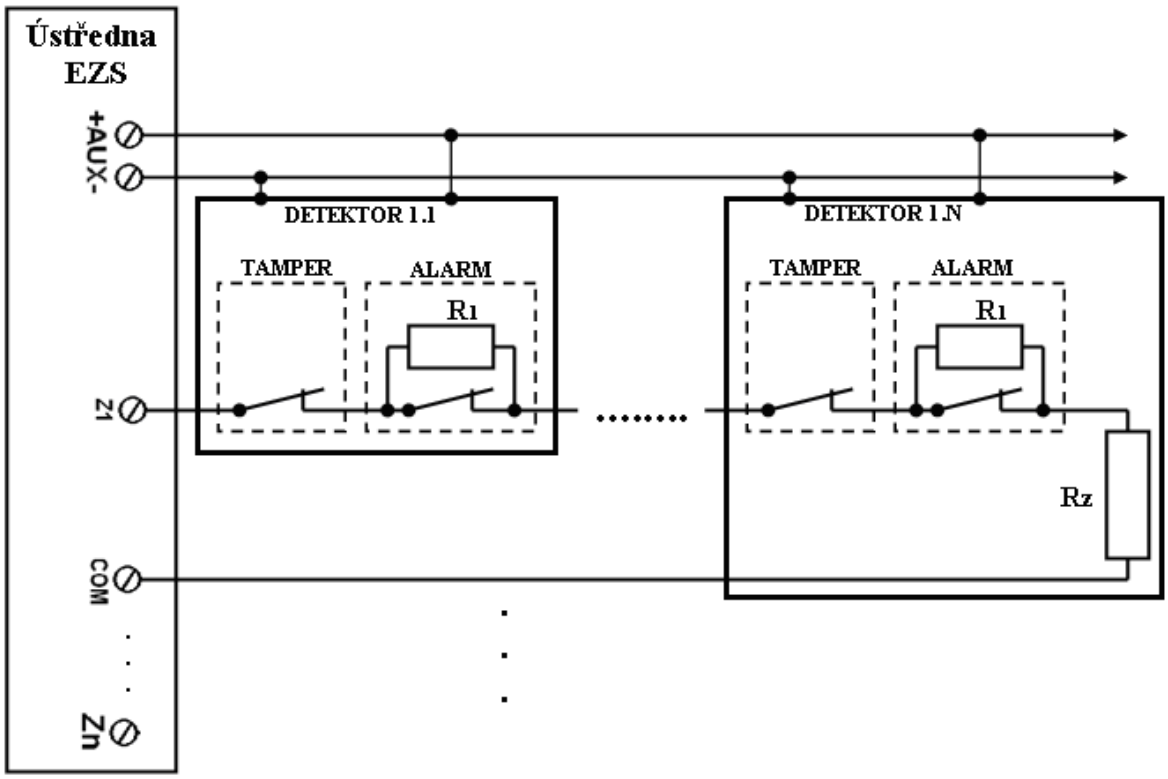
4.2.3 NC dvojitě vyvážená

Výhoda zapojení NC dvojitě vyvážená proti NC jednoduše vyvážená spočívá v tom, že pomocí dalšího odporu R_1, který je připojen paralelně ke kontaktu alarm, lze odlišit vyvolání poplachu pomocí kontaktu alarm od kontaktu tamper. Počet stavů se zvýšil na 4 a je znázorněn na obr. 9. Schéma zapojení znázorňuje obr. 10.



Obrázek 9. Vyhodnocení stavu zóny v závislosti na hodnotě odporu smyčky typu NC – dvojitě vyvážená

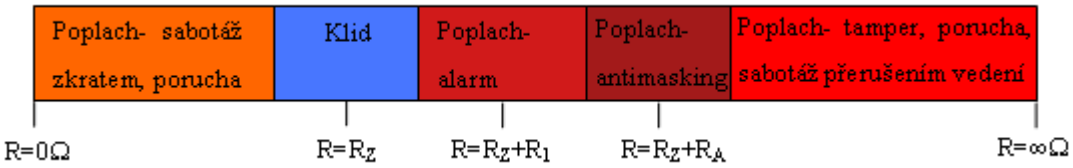
Jedinou nevýhodou je chybějící detekce zakrytí detektoru. Hodnota odporu R_1 je různá a udává ji výrobce.



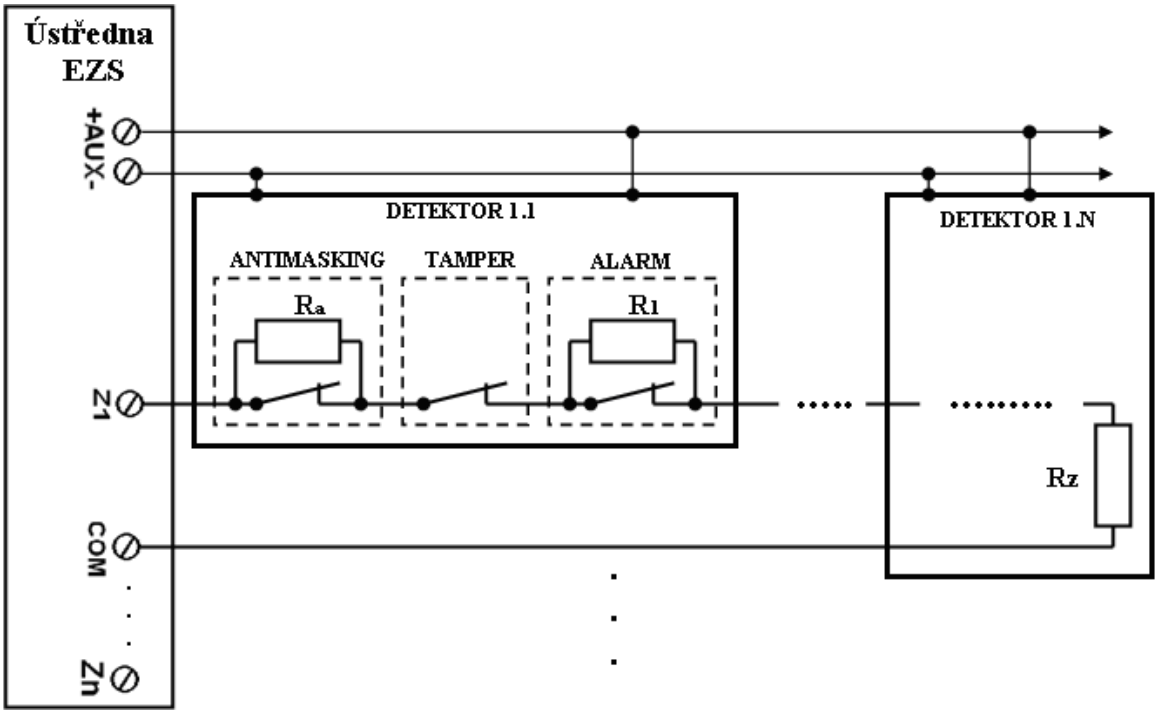
Obrázek 10. Schéma zapojení smyčky typu NC – dvojitě vyvážená

4.2.4 NC trojitě vyvážená

Vylepšení proti zapojení NC dvojitě vyvážená spočívá v přidání kontaktu antimasking a dalšího odporu R_A, který je připojen paralelně ke kontaktu antimasking a který umožní detekci zakrytí detektoru. Jedná se o nejvhodnější zapojení, kde proti NC dvojitě vyvážená přibyl další stav, který nastává při hodnotě odporu vedení $R=R_Z+R_A$. Zde se jedná o poplach z důvodu zamaskování scény. Zapojení má 5 stavů, které jsou znázorněny na obr. 11. Hodnota odporu R_A závisí na výrobci (zpravidla 12 KΩ).



Obrázek 11. Vyhodnocení stavu zóny v závislosti na hodnotě odporu smyčky typu NC – trojitě vyvážená

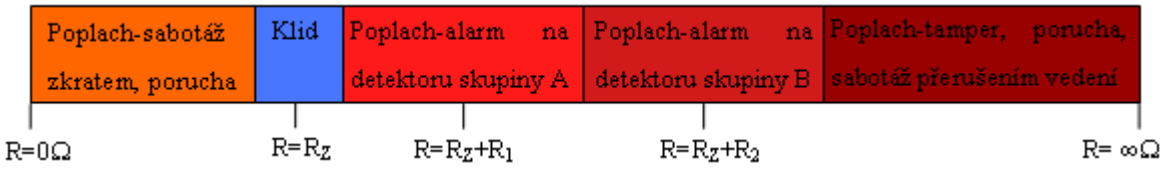


Obrázek 12. Schéma zapojení smyčky typu NC trojitě vyvážená

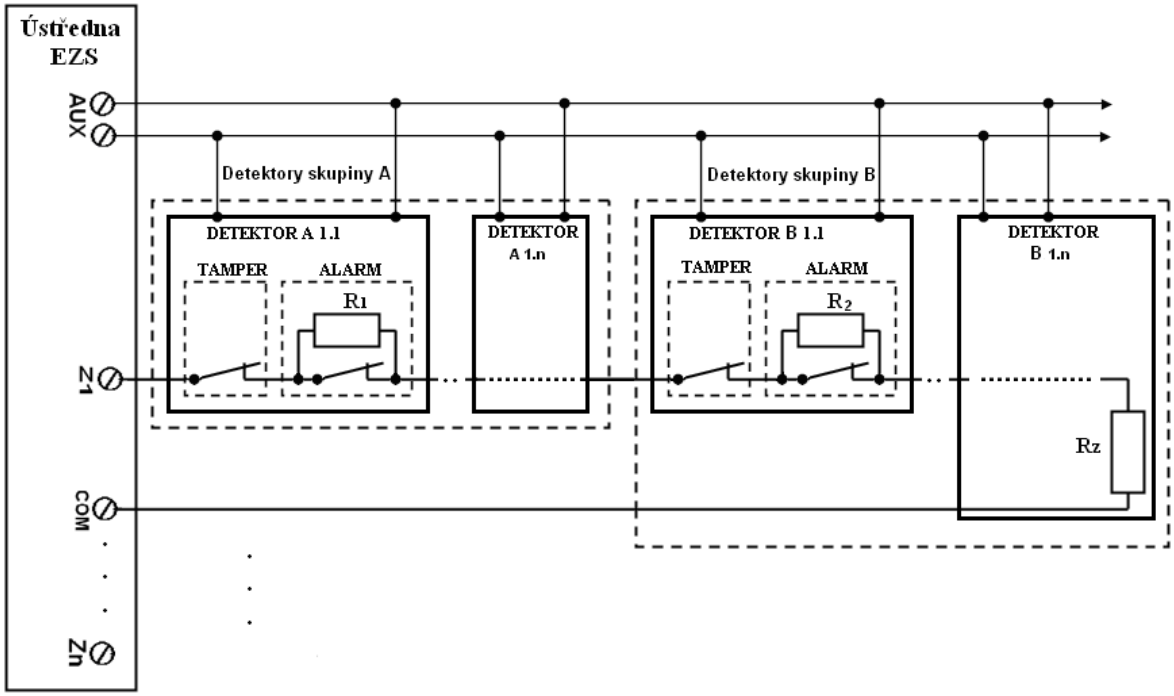
4.2.5 NC zdvojení zón (ATZ)

V praxi se často používá zdvojení zón pro přesnější identifikaci místa narušení objektu v jedné smyčce. Detektory se zde rozdělí do dvou skupin na „detektory skupiny A“ a

„detektory skupiny B“. „Detektory skupiny A“ používají pro vyhodnocení poplachu odpor R_1 a „detektory skupiny B“ používají odpor R_2. Všechny detektory jsou připojeny do jedné smyčky, ale ústředna indikuje narušení objektu pomocí dvou zón v závislosti na odporu smyčky. Jestliže je celkový odpor roven přibližně R_Z (hodnotě zakončovacího odporu), jsou obě zóny ve stavu „klid“ a není vyhlášen poplach. Je-li celkový odpor mnohem menší než R_Z, jedná se o sabotáž zkratem nebo poruchu. Platí-li přibližně $R=R_Z+R_1$, je vyhlášen poplach v první skupině detektorů, a platí-li $R=R_Z+R_2$, je vyhlášen poplach v druhé skupině detektorů. Při celkovém odporu výrazně převyšujícím $R=R_Z+R_2$ se jedná o poruchu, sabotáž přerušením vedení nebo narušení krytu detektoru pomocí kontaktu tamper. Hodnota odporu R_2 opět závisí na výrobci. Samozřejmě zde nechybí zakončovací odpor pro vyhodnocení sabotáže zkratem.



Obrázek 13. Vyhodnocení stavu zóny v závislosti na hodnotě odporu smyčky typu NC-ATZ



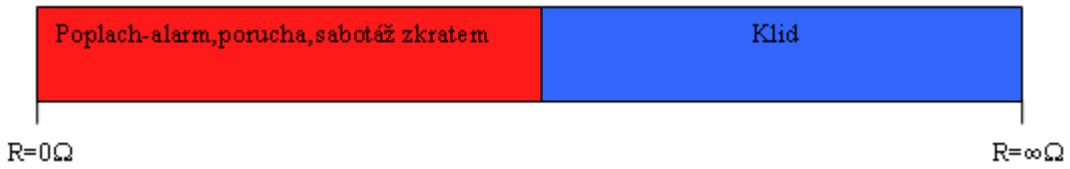
Obrázek 14. Schéma zapojení smyčky typu NC-ATZ

4.3 Možnosti zapojení drátových smyček typu NO (normally opened)

Detektory typu NO (normally opened) jsou naopak ve stavu „klid“, jestliže jsou kontakty v detektoru rozepnuty. Stav „poplach“ nastane v případě, že se některý kontakt v detektoru sepne. Jedná se o spínací kontakt.

4.3.1 NO (normally opened)

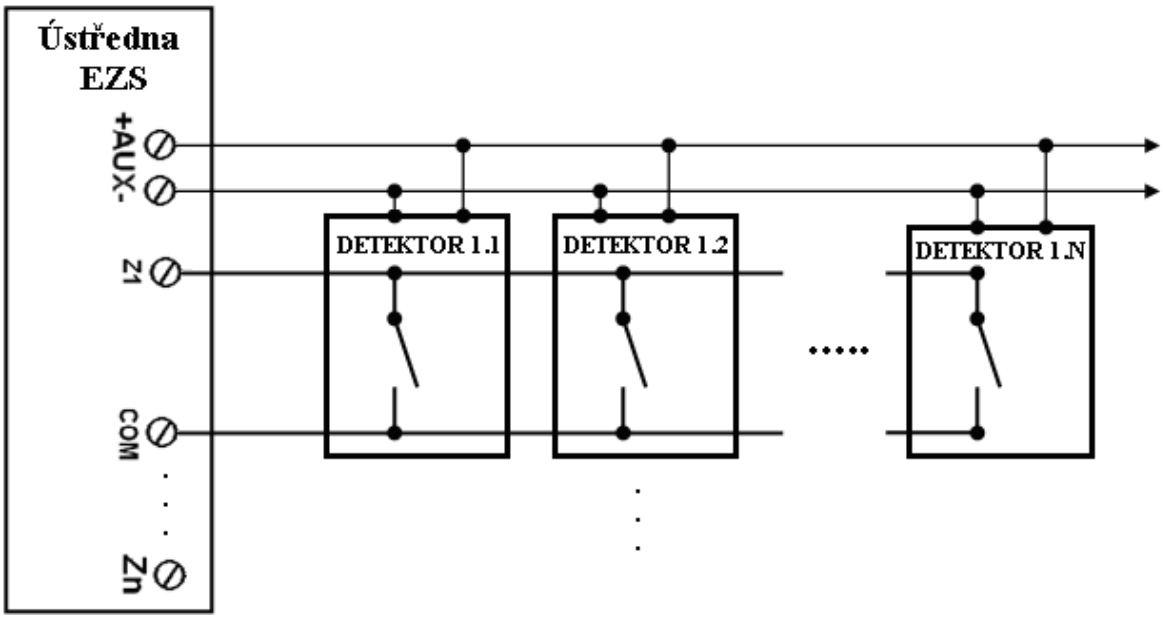
Detektory jsou řazeny paralelně (mimo zapojení ATZ) a jejich doporučený počet na jedné zóně je 5. Ústředna zde vyhodnotí jen dva stavy. Jestliže jsou kontakty detektorů rozepnuty, je odpor smyčky velký a zóna je ve stavu „klid“. Při sepnutí kontaktů je naopak odpor smyčky velmi malý a ústředna je ve stavu „poplach“.



Obrázek 15. Vyhodnocení stavu zóny v závislosti na hodnotě

odporu vedení smyčky typu NO (normally opened)

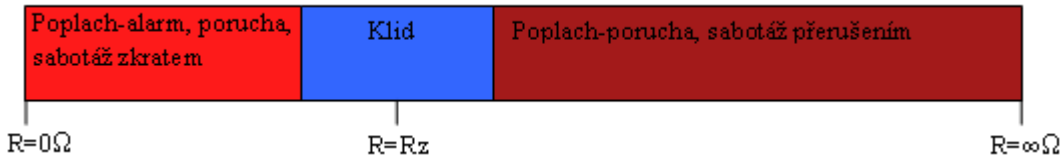
Z důvodu možnosti sabotáže pomocí přerušení vedení se uvedené zapojení nesmí používat. V zapojení dále chybí kontakt tamper a kontakt antimasking.



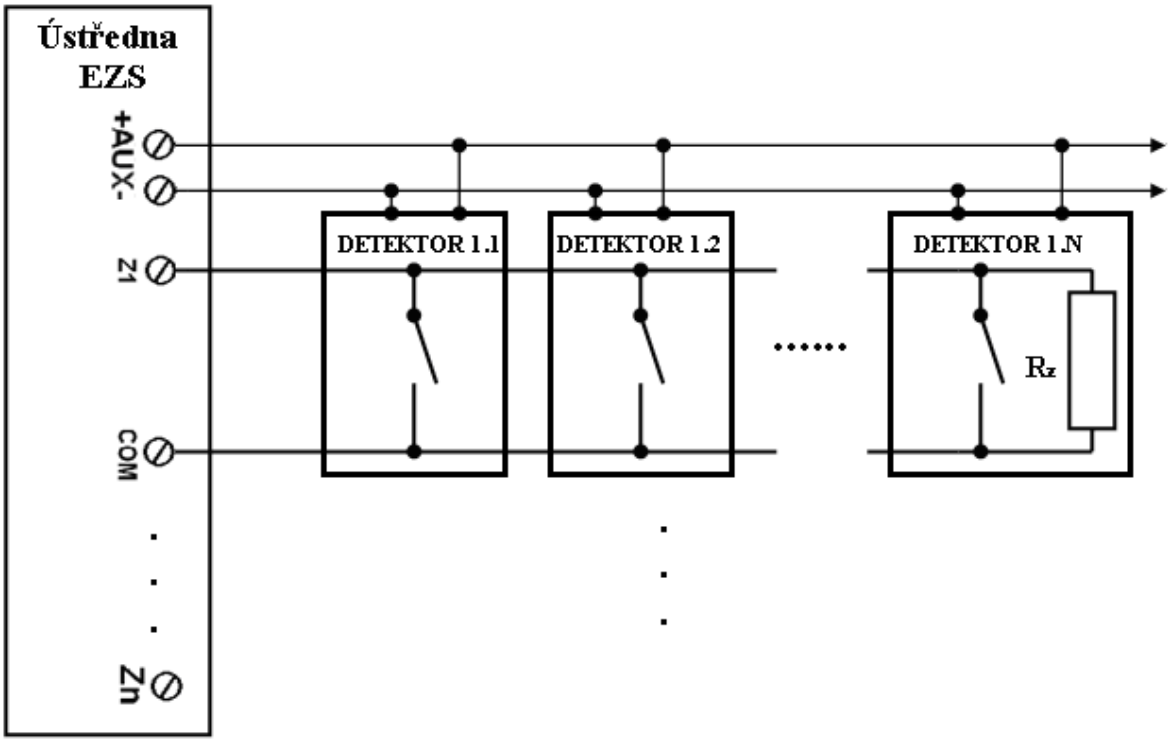
Obrázek 16. Schéma zapojení smyček typu NO (normally opened)

4.3.2 NO jednoduše vyvážená

Detektory jsou opět zapojeny paralelně. Hlavní výhodou proti předchozímu zapojení je v použití zakončovacího odporu, který chrání smyčku před sabotáží pomocí přerušení vedení i zkratování. Využití je pro detektory i požární hlásiče (ionizační, optický, teplotní nebo kombinované). Díky NO jednoduše vyvážená lze vyhodnotit celkem tři stavy. Jestliže se odpor zóny blíží odporu Rz (zakončovací odpor), zóna je ve stavu „klid“. Při přerušení vedení je vyhlášen poplach z důvodu sabotáže rozpojení vedení a blíží-li se odpor zóny nule, tak je vyhlášen poplach z důvodu sabotáže zkratem nebo spuštění alarmu detektorem. Hlavní chybou zapojení typu NO jednoduše vyvážena je v chybějícím kontaktu tamper a antimasking. [6]



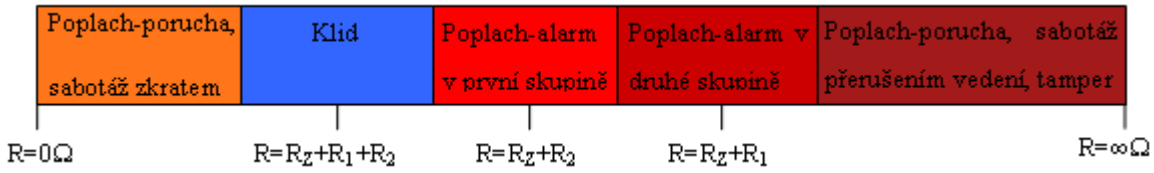
Obrázek 17. Vyhodnocení stavu zóny v závislosti na hodnotě odporu vedení smyčky typu NO-jednoduše vyvážená



Obrázek 18. Schéma zapojení smyček typu NO – jednoduše vyvážená

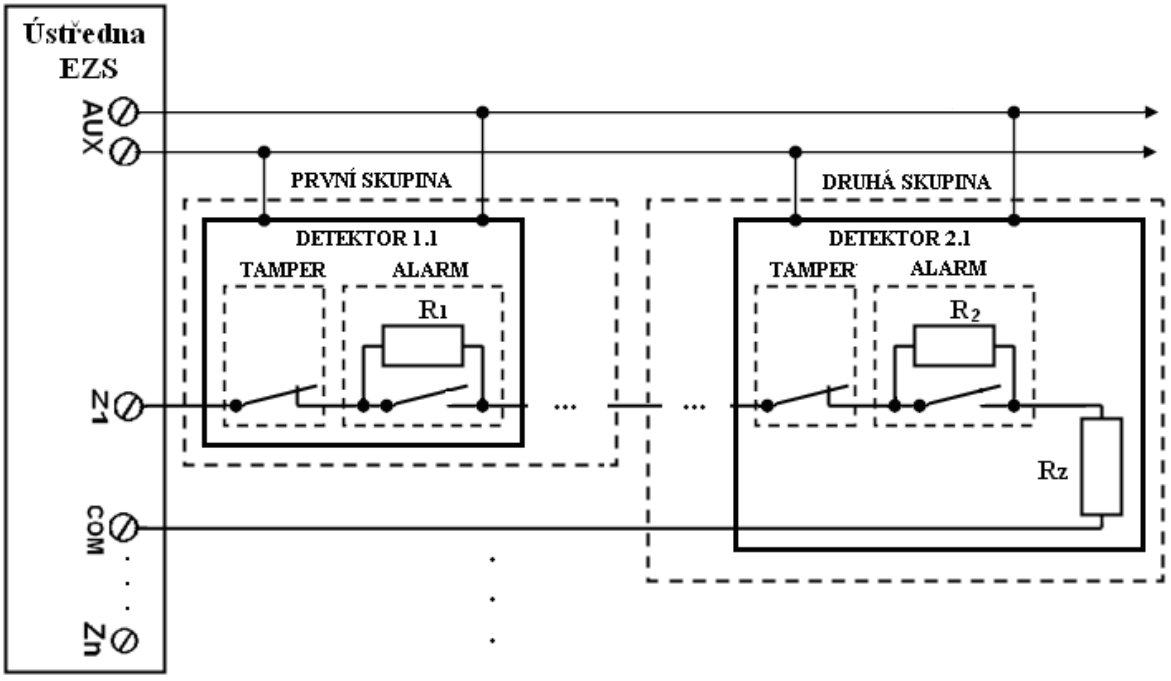
4.3.3 NO zdvojení zón (ATZ)

Využití je pro přesnější identifikaci místa narušení objektu. Díky odporům R_1 a R_2 se rozdělí detektory do dvou skupin. V první skupině se použije odpor R_1 a v druhé odpor R_2. Všechny detektory jsou připojeny na jednu smyčku, ale při použití zdvojení zón ústředna indikuje narušení objektu pomocí dvou zón v závislosti na odporu smyčky. Zapojení je schopno rozpoznat pět stavů. Blíží-li se odpor smyčky odporu R_Z (zakončovací odpor), ústředna je ve stavu „klid“. Bude-li hodnota odporu blízká nekonečnu, tak se jedná o sabotáž přerušením vedení, poruchu nebo neoprávněnou manipulaci s krytem. Sabotáž zkratem je vyhlášena při velmi malém odporu zóny (blízkém nule). Je-li celkový odpor smyčky přibližně $R=R_Z+R_2$, je vyhlášen poplach v první skupině detektorů. Rovná-li se celkový odpor přibližně $R=R_Z+R_1$, je vyhlášen poplach v druhé skupině detektorů.



Obrázek 19. Vyhodnocení stavu zóny v závislosti na hodnotě odporu vedení smyčky typu NO-ATZ

Nevýhodou je chybějící detekce zamaskování scény (antimasking).



Obrázek 20. Schéma zapojení smyček typu NO-ATZ

5 CITACE Z NORMY ČSN EN 50131, KTERÁ SE ZABÝVÁ OCHRANOU PROTI SABOTÁŽI

5.1 Stupně zabezpečení

I&HAS musí být přiřazen stupeň zabezpečení, určující jeho provedení. Musí být zařazen do jednoho ze čtyř stupňů, přičemž nejnižší je stupeň 1 a nejvyšší stupeň 4. Stupeň zabezpečení I&HAS musí odpovídat komponentu s nejnižším stupněm zabezpečení.

Stupeň 1: Nízké riziko

Předpokládá se, že vetřelec nebo lupič mají malou znalost I&HAS a mají k dispozici omezený sortiment snadno dostupných nástrojů.

Stupeň 2: Nízké až střední riziko

Předpokládá se, že vetřelec nebo lupič mají omezené znalosti I&HAS a používání běžného nářadí a přenosných přístrojů.

Stupeň 3: Střední až vysoké riziko

Předpokládá se, že vetřelec nebo lupič jsou obeznámeni s I&HAS a mají rozsáhlý sortiment nástrojů a přenosných elektronických zařízení.

Stupeň 4: Vysoké riziko

Používá se, má-li zabezpečení prioritu před všemi ostatními hledisky. Předpokládá se, že vetřelec nebo lupič jsou schopni nebo mají možnost zpracovat podrobný plán vniknutí a mají kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících komponentů I&HAS. [1]

5.2 Ochrana proti sabotáži

Komponenty I&HAS musí mít prostředky zamezující přístup k jejich vnitřním součástkám, aby bylo minimalizováno riziko sabotáže. Požadavky na ochranu proti sabotáži se mohou lišit podle stupně I&HAS a podle toho, zda je komponent I&HAS umístěn uvnitř nebo vně střeženého prostoru. [1]

5.3 Detekce sabotáže

Komponenty I&HAS specifikované v obr. 21 musí být vybaveny prostředky pro detekci sabotáže. Obr. 22 specifikuje typy sabotáže, které je třeba detekovat. Detekce sabotáže musí být ve všech stupních zabezpečení funkční ve stavu střežení i klidu.

Doplňkové ovládací zařízení určené k instalaci vně střeženého prostoru musí obsahovat prostředky zamezující záměnu tohoto zařízení a/nebo signálů a zpráv mezi doplňkovým ovládacím zařízením a ústřednou. Tento požadavek nemusí být uplatněn, jestliže jakákoli takováto záměna nemůže ovlivnit správnou funkci I&HAS. [1]

5.3.1 Komponenty na něž se detekce sabotáže vztahuje

Komponenty	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Ústředna/doplňkové ovládací zařízení [a]/komunikátor střeženého objektu/výstražné zařízení/napájecí zdroj	P	P	P	P
Tísňové prostředky [a]	V	P	P	P
Detektory narušení [b]	V	P	P	P
Rozvodné krabice [c]	V	V	P	P
Klíč: V = volitelné P = povinné.				
[a] Přenosné tísňové prostředky nemusí vyhovovat požadavkům této tabulky.				
[b] Je akceptováno, že může být problematické realizovat detekci sabotáže u mechanicky nebo magneticky aktivovaných spínačů. U některých stupňů zabezpečení však může být nezbytné chránit magneticky aktivované spínače proti sabotáži pomocí vnějšího magnetického nebo elektromagnetického zdroje.				
[c] Má-li I&HAS ochranu proti záměně signálů nebo zpráv, není třeba u stupňů 1, 2 a 3 opatřovat rozvodné krabice detekcí sabotáže.				

Obrázek 21. Komponenty na něž se detekce sabotáže vztahuje [7]

5.3.1.1 Ústředna (control and indicating equipment)

Zařízení pro příjem, zpracování, ovládání, indikaci a iniciaci následného přenosu informace.

5.3.1.2 Doplňkové ovládací zařízení (ancillary control equipment)

Zařízení použité pro doplňkové ovládací účely.

Doplňkovým ovládacím zařízením se rozumí například klávesnice, biometrický prvek, čtečka karet nebo klíčenek apod., umístněné vně střeženého prostoru, pomocí něhož je možné zařízení uvádět do stavu střežení nebo klidu, případně jímž se může ukončovat proces uvedení do stavu střežení nebo zahajovat proces uvedení do stavu klidu. [1]

5.3.1.3 Komunikátor střeženého objektu (supervised premises transceiver)

Zařízení ve střeženém objektu, obsahující rozhraní k I&HAS a k poplachové přenosové síti. Poplachové přenosové sítě jsou sítě, používané k přenosu z jednoho nebo více I&HAS do jednoho nebo více poplachových přijímacích center.

5.3.1.4 Výstražné zařízení (warning device)

Zařízení, které produkuje zvukový poplachový signál v odezvě na hlášení poplachu. [7]

5.3.1.5 Napájecí zdroj (power supply)

Část I&HAS, zajišťující energii pro napájení I&HAS.

5.3.1.6 Tísňový prostředek (hold-up device)

Zařízení, jehož aktivací je generován poplachový signál nebo zpráva.

5.3.1.7 Detektor narušení (intrusion detector)

Zařízení konstruované ke generování signálu nebo zprávy o vniknutí, jako reakci na nenormální stav detekující přítomnost nebezpečí. [1]

5.3.1.8 Rozvodné krabice

Zařízení určené ke zřizování odbočných míst v poplachových zabezpečovacích systémech. [8]

5.3.2 Jaká sabotáž musí být detekována

Způsoby	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Otevření normálním způsobem	P	P	P	P
Odejmutí z montážní plochy – bezdrátové komponenty I&HAS	V	P	P	P
Odejmutí z montážní plochy – komponenty I&HAS připojené kabelem	V	V	P[c]	P
Narušení do akustického výstražného zařízení	V	V	V	P[a]
Narušení do ústředny/doplňkového ovládacího zařízení/poplachového přenosového systému	V	V	V	P[a]
Změna orientace detektoru	V	V	P[b]	P[b]
Klíč: V = Volitelné P = Povinné.				
[a] Vztahuje se na CIE, ACE, SPT nebo WD, jsou-li umístěny vně střežených prostorů. [b] Je-li změna orientace možná. [c] Tento požadavek je volitelný pro rozvodné krabice a kontakty otevření (magnetické).				

Obrázek 22. Jaká sabotáž musí být detekována [7]

CIE – Ústředna I&HAS (control and indicating equipment)

ACE- Doplňkové ovládací zařízení (ancillary control equipment)

SPT – Komunikátor střeženého objektu (supervised premises transceiver)

WD – Výstražné zařízení (warning device) [1]

5.3.3 Monitorování záměny

V závislosti na stupni I&HAS musí být zajištěno monitorování, umožňující detekovat záměnu komponentů I&HAS. Monitorování musí splňovat požadavky obr. 23. Je-li I&HAS ve stavu střežení nebo klidu a dojde k detekci záměny, musí být generován signál nebo zpráva sabotáže.

Požadavky na monitorování	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Záměna komponentů I&HAS	V	V	V	P
Klíč: V = Volitelné P = Povinné.				

Obrázek 23. Monitorování záměny [1]

5.3.4 Časové závislosti činnosti I&HAS

Zpracovány musí být signály vniknutí, tísně a sabotáže, trvající déle než 400 ms. Poruchové signály musí být zpracovány, trvají-li déle než 10 s. [1]

5.4 Rozbor požadavků norem PZS na detekci sabotáže

Z normy ČSN EN 50131 vyplývá, že se musí střežit ústředna, doplňkové ovládací zařízení, komunikátor střeženého objektu, výstražné zařízení, napájecí zdroj, tísňové prostředky, detektory narušení a rozvodné krabice v závislosti na stupni zabezpečení a způsobu sabotáže. Povinnost střežení komponent v závislosti na stupni zabezpečení znázorňuje obr. 21. Způsob sabotáže, který musí být detekován v závislosti na stupni zabezpečení, znázorňuje obr. 22. Ve čtvrtém stupni se dále musí detekovat záměna komponentů I&HAS, proto se drátové ústředny typu NO a NC nesmí použít pro čtvrtý stupeň zabezpečení.

Signály tísně, sabotáže a vniknutí musí byt zpracovány, trvají-li déle, než 400 ms. Poruchové signály musí být zpracovány, trvají-li déle, než 10 s.

5.4.1 Komponenty na které se vztahuje povinnost detekce sabotáže

5.4.1.1 Stupeň 1

V prvním stupni je povinností detekovat sabotáž v ústředně, doplňkovém ovládacím zařízení, komunikátoru střeženého objektu, výstražném zařízení a napájecím zdroji.

5.4.1.2 Stupeň 2

Ve druhém stupni je povinností detekovat sabotáž v ústředně, doplňkovém ovládacím zařízení, komunikátoru střeženého objektu, výstražném zařízení, napájecím zdroji, tísňových prostředcích a detektorech narušení.

5.4.1.3 Stupeň 3

V třetím stupni je povinností detekovat sabotáž v ústředně, doplňkovém ovládacím zařízení, komunikátoru střeženého objektu, výstražném zařízení, napájecím zdroji, tísňových prostředcích, detektorech narušení a rozvodných krabicích.

5.4.1.4 Stupeň 4

Ve čtvrtém stupni je povinností detekovat sabotáž v ústředně, doplňkovém ovládacím zařízení, komunikátoru střeženého objektu, výstražném zařízení, napájecím zdroji, tísňových prostředcích, detektorech narušení a rozvodných krabicích.

5.4.2 Způsob sabotáže, který musí byt detekován

5.4.2.1 První stupeň

V prvním stupni je povinnost detekovat pouze sabotáž pomocí otevření normálním způsobem. Využívá se při zabezpečování objektů s malými aktivy (chaty, garáže).

5.4.2.2 Druhý stupeň

Ve druhém stupni je povinnost detekovat otevření normálním způsobem a u bezdrátových komponentů i odejmutí z montážní plochy. Využívá se pro kancelářské prostory, komerční prostory a obytné objekty.

5.4.2.3 Třetím stupeň

Ve třetím stupni je povinností detekovat otevření normálním způsobem, odejmutí z montážní plochy u bezdrátových komponent i komponent připojené kabelem a je-li to možné i změna orientace detektoru. Využití třetího stupně je například pro banky.

5.4.2.4 Čtvrtý stupeň

Ve čtvrtém stupni musí být detekovány všechny způsoby sabotáže jako ve třetím stupni, ale přibývá zde povinnost detekce narušení do akustického výstražného zařízení, ústředny, doplňkového ovládacího zařízení a poplachového přenosového systému. Používá se u muničních skladů a objektů s tajnými archívy.

II. PRAKTICKÁ ČÁST

6 ZÁKLADNÍ PARAMETRY A PROGRAMOVÁNÍ ÚSTŘEDNY SPECTRA 1728 OD FIRMY PARADOX SECURITY SYSTEMS

Pro testování bezpečnosti drátových ústředen jsem zvolil ústřednu Spectra 1728, protože díky možnosti zvolení rychlosti zóny již od 10 ms se jedná o nejvhodnější ústřednu pro testování. V následující části jsou uvedeny základní parametry ústředny a úryvky z instalačního manuálu, které je potřeba umět a znát pro pochopení logiky programování ústředny.

6.1 Základní parametry

- Možnost připojení až 10 zón (s ATZ)
- Bus sběrnice pro možnost připojení klávesnice a rozšiřujících modulů
- PGM výstup
- Telefonní komunikátor pro možnost připojení na PCO
- Možnost nastavit rychlost zóny
- Možnost vyvolání poplachu pomocí zkratek Panik
- Výstup pro sirénu
- Až 48 uživatelských kódů
- Systém lze rozdělit do dvou nezávislých systémů
- Zjištění poruch pomocí TBL
- Paměť událostí
- Náhradní baterie (12V)

6.2 Zobrazení poruch

LED #	POPIS	DETAILY
[1]	Porucha baterie	Ústředna testuje baterii dynamicky každých 60 sekund. Tato porucha indikuje, že záložní baterie je odpojena, nebo že její kapacita neumožňuje zálohovat systém při výpadku sítě. Tento stav je také indikován, je . li napětí na baterii nižší než 10,5 V. v tom případě je nutné akumulátor dobít nebo vyměnit.
[2]	Porucha baterie bezdrátu	Tento stav je indikován, klesne – li napětí bezdrátového vysílače pod povolenou hranici. Současně poruchu indikuje LED na vysílači. Baterii je nutno vyměnit za nové.
[3]	Výpadek sítě	Nastane – li tato porucha, zhasne na klávesnici LED s označením AC. Ústředna přenese komunikátorem zprávu, programovanou v sekci [205]. Tato zpráva může být zpožděna o hodnotu programovanou na adrese [086].
[4]	Siréna nevyvážena	Tato porucha indikuje nevyvážení výstupu BELL. Pokud výstupy nepoužíváme (není zde připojena siréna), je nutné vyvážit svorky 1kΩ odporem.
[5]	Siréna přetížena	Sirénový výstup se automaticky odpojí, jestliže odebíraný proud překročí3A. Tato porucha může nastat pouze při poplachu.
[6]	Napájecí výstup AUX přetížen	Napájecí výstup je chráněn elektronickou pojistkou, která tento výstup odpojí, přesáhne – li odebíraný proud hodnoty 1,1A. Po uklidnění se sama vrátí do původního stavu.
[7]	Chyba komunikace	Tato porucha vznikne, nedojde – li ke spojení s PCO do vyčerpání všech pokusů o spojení.
[8]	Vynulování vnitřních hodin	Tato porucha nastane vždy při zapnutí ústředny k napájení. Ppro nastavení hodin stiskneme klávesu [8] a zadáme čas v režimu zobrazení 24 hod.
[9]	Tamper / porucha kabeláže zóny	Tato porucha může nastat, le – li povoleno sledování ochranného kontaktu. Porucha indikuje problém s kabeláží na jedné nebo více zónách, nebo otevření krytu bezdrátových vysílačů. Pokud má ústředna indikovat zkrat na zóně, musí být zóny definovány se zakončovacím odporem. Po stisku klávesy [9] se zobrazí konkrétní zóna. Zadáním instalačního kódu zrušíte poruchu tamperu-
[10]	Porucha telefonní linky	Tato porucha je zobrazena v případě odpojení telefonní linky na déle než 30 sekund.
[STAY] nebo [11]	Porucha požární smyčky	Stejné jako porucha kabeláže, platí však pouze pro zónu 3, je – li programována jako zóna požární.
[FORCE] nebo [16]	Porucha klávesnice	Jestliže dojde k poruše komunikace mezi ústřednou a klávesnicí, začne blikat klávesa [TRBL] a klávesa [FORCE] začne svítit a klávesnice pípá v intervalu 5s. Pípání umlkne po stisku libovolné klávesy. Po obnovení komunikace se systém vrátí do původního stavu.
[BYP] nebo [12]	Ztráta modulu	Porucha nastane, nedojde –li dlouhou dobu ke komunikaci mezi modulem a ústřednou.
[MEM] nebo [13]	Ztráta bezdrátového modulu	Porucha nastane, nedojde –li dlouhou dobu ke komunikaci mezi bezdrátovým vysílačem a přijímačem. Po stisku klávesy [MEM] klávesnice, zobrazí o kterou zónu se jedná.

Obrázek 24. Zobrazení poruch u ústředny Spectra [10]

6.3 Programování zón

Programování zón se provádí podle následujícího postupu.

1. Stiskni [ENTER]

2. Zadej [instalační kód]

3. Zadej tři číslice programovací [sekce]

4. Zadej jednu číslici TYP ZÓNY

5. Zadej jednu číslici pro přiřazení skupině

6. Zvol parametr (y) zóny

7. Stiskni [ENTER]

Instalační kód je implicitně nastaven na hodnotu 0000. [10]

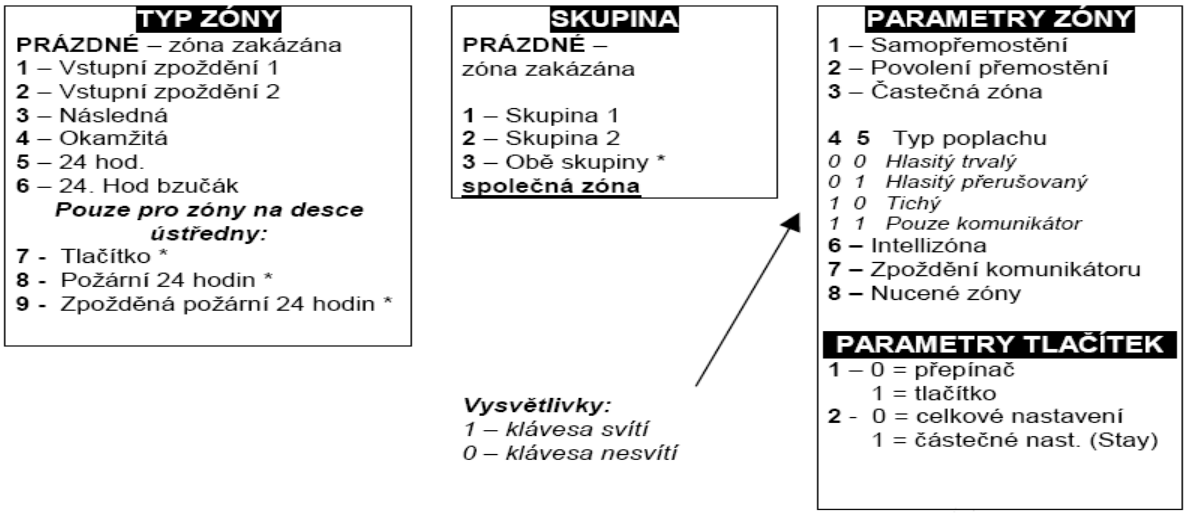
6.3.1 Programovací sekce v rozsahu 001-016

Pomocí programovací sekce v rozsahu 001-016 určíme, kterou zónu budeme programovat. Situaci znázorňuje obr. 25.

SEKCE	POPIS	TYP ZONY	SKUPINA	PARAMETRY
[001] = Zóna 1:	_____	____	____	1 2 3 4 5 6 7 8
[002] = Zóna 2:	_____	____	____	1 2 3 4 5 6 7 8
[003] = Zóna 3:	_____	____	____	1 2 3 4 5 6 7 8
[004] = Zóna 4:	_____	____	____	1 2 3 4 5 6 7 8
[005] = Zóna 5:	_____	____	____	1 2 3 4 5 6 7 8
[006] = Zóna 6:	_____	____	____	1 2 3 4 5 6 7 8
[007] = Zóna 7:	_____	____	____	1 2 3 4 5 6 7 8
[008] = Zóna 8:	_____	____	____	1 2 3 4 5 6 7 8
[009] = Zóna 9:	_____	____	____	1 2 3 4 5 6 7 8
[010] = Zóna 10:	_____	____	____	1 2 3 4 5 6 7 8
[011] = Zóna 11:	_____	____	____	1 2 3 4 5 6 7 8
[012] = Zóna 12:	_____	____	____	1 2 3 4 5 6 7 8
[013] = Zóna 13:	_____	____	____	1 2 3 4 5 6 7 8
[014] = Zóna 14:	_____	____	____	1 2 3 4 5 6 7 8
[015] = Zóna 15:	_____	____	____	1 2 3 4 5 6 7 8
[016] = Zóna 16:	_____	____	____	1 2 3 4 5 6 7 8
	Výchozí hodnoty =	*prázdné*	*1*	*1 2 . . . . . .*

Obrázek 25. Programovací sekce 001-016 u ústředny Spectra [10]

6.3.2 Nastavení typu zóny, skupiny a parametrů zóny



Obrázek 26. Nastavení typu zóny, skupiny a parametrů zóny u ústředny Spectra [10]

Na obr. 26 je popsána funkce ústředny v závislosti na nastavení.

6.3.2.1 Vysvětlení jednotlivých zkratek

Vstupní zpoždění 1 a 2: Zóny, které vyhlásí poplach při narušení v zabezpečeném stavu až po uplynutí příchodové doby. Existují dva typy zpoždění pro možnost použití dvou rozdílných časů, například pro obě skupiny s rozdílnými příchodovými trasami. Tyto časy nemají souvislost s jednotlivými skupinami, lze je požít nezávisle.

Následná: Tato zóna generuje poplach při narušení okamžitě. Probíhá – li však na systému již vstupní zpoždění (byla narušena zpožděná zóna), chová se tato smyčka jako zpožděná. Použití: uprostřed vstupní trasy.

Okamžitá: Tato zóna způsobí při nastaveném systému poplach okamžitě.

Tlačítko: Definujeme – li zónu jako tlačítko, lze její pomocí nastavovat / odstavovat systém. Tlačítko je vždy zapojeno jako jednoduchá zóna (bez zdvojení - v klidu 1 KΩ, při aktivaci 0 Ω, pokud používáme zdvojené zóny, tak jako tlačítko naprogramujeme první zónu ve zdvojení, druhou zónu nelze použít).

Požární: Zóna pro připojení požárních detektorů. U verzí 1.2x může být jako požární zóna definovaná pouze zóna číslo 3, přiřadíme – li ji definici 5 (24 hod). Přiřadíme-li zóně 3 u této verze definici 6, stane se požární zpožděnou zónou.

Požární zpožděná: Po aktivaci této zóny je aktivována siréna. Po 30 sekundách dojde k dalšímu otestování zóny, je-li uzavřena nebo je-li zadán kód, dojde ke zrušení poplachu.

24 Hodinová: Tato zóna způsobí poplach okamžitě bez ohledu na to, zdali je systém nastaven.

24 Hodinová bzučák: Tato zóna aktivuje bzučák klávesnice (bez sirény) okamžitě bez ohledu na to, zdali je systém nastaven. Bzučák umlčíme zadáním platného kódu.

Přiřazení skupině: Zónu přiřadíme skupině jedna nebo dvě, podle toho, do kterého prostoru má náležet. Stav zóny se v druhém systému neprojeví.

Společné zóny: Přiřadíme–li zónu oběma skupinám vznikne klasická společná zóna. Jsou-li nastaveny obě skupiny je nastavena také, je-li alespoň jedna skupina odstavena, je odstavena také. Tato funkce není aktivní u verzí 1.2x.

Samopřemostění: Pokud počet opakování poplachu během jednoho nastavení přesáhne počet, programovaný na adrese [089], zóna se sama přemostí.

Povolení přemostění: Pouze tyto zóny lze přemostit (manuálně i automaticky).

Stay: Tyto zóny nebudou při částečném nastavení ve střežení (budou automaticky přemostěny).

Intelli zóny: Tyto zóny vyhlásí poplach pouze tehdy, jsou – li narušeny během doby, naprogramovaný na adrese [084] dvakrát, nebo jsou–li během, této doby narušeny dvě Intelli zóny. [10]

6.4 Povolení zakončovacího odporu na smyčce

Postupuje se podle postupu zmíněného v kapitole 6.3. Jako sekce se zadá číslo 132 a dále stačí pouze zmáčknout číslo 4 a enter. Rozsvícení indikuje aktivaci.

6.5 Nastavení rychlosti zóny

Při programování rychlosti zóny se postupuje podle kapitoly 6.3. Jako sekce se zvolí 050-065 v závislosti na zóně, kterou chceme programovat. Následují tři číslice pro stanovení rychlosti zóny. Při vynásobení 10 ms dostaneme skutečnou rychlost zóny.

6.5.1 Programovací sekce 050-065

Nastavením sekce 050-065 zvolíme, u které zóny nastavujeme rychlost vyhodnocení viz obr. 27.

Sekce	Desítková hodnota (000 - 255)	Popis	Tovární hodnota
[050]	__/__/__ x 10 ms	Rychlost zóny (zóna 1)	600 ms
[051]	__/__/__ x 10 ms	Rychlost zóny (zóna 2)	600 ms
[052]	__/__/__ x 10 ms	Rychlost zóny (zóna 3)	600 ms
[053]	__/__/__ x 10 ms	Rychlost zóny (zóna 4)	600 ms
[054]	__/__/__ x 10 ms	Rychlost zóny (zóna 5)	600 ms
[055]	__/__/__ x 10 ms	Rychlost zóny (zóna 6)	600 ms
[056]	__/__/__ x 10 ms	Rychlost zóny (zóna 7)	600 ms
[057]	__/__/__ x 10 ms	Rychlost zóny (zóna 8)	600 ms
[058]	__/__/__ x 10 ms	Rychlost zóny (zóna 9)	600 ms
[059]	__/__/__ x 10 ms	Rychlost zóny (zóna 10)	600 ms
[060]	__/__/__ x 10 ms	Rychlost zóny (zóna 11)	600 ms
[061]	__/__/__ x 10 ms	Rychlost zóny (zóna 12)	600 ms
[062]	__/__/__ x 10 ms	Rychlost zóny (zóna 13)	600 ms
[063]	__/__/__ x 10 ms	Rychlost zóny (zóna 14)	600 ms
[064]	__/__/__ x 10 ms	Rychlost zóny (zóna 15)	600 ms
[065]	__/__/__ x 10 ms	Rychlost zóny (zóna 16)	600 ms

Obrázek 27. Nastavení rychlosti zóny u ústředny Spectra [10]

6.6 Programování uživatelských kódů

1. Stiskneme klávesu [ENTER]

2. Zadáme [SYSTÉMOVÝ MASTER KÓD] nebo [MASTER KÓD]

3. Zadáme 3 číslice sekce (viz dále)

4. Zadáme 4 nebo 6 číslic číselné kombinace kódu

Master kód je z výroby nastaven na 1234.

6.6.1 Mazání uživatelských kódů

1. Postupujeme stejně jako v předchozím případě v bodech 1 – 3.

2. Stiskneme klávesu [FORCE] pro každou číslici kódu (4 - krát

nebo 6 – krát), dokud klávesnice nevydá potvrzovací pípnutí. [10]

6.6.2 Vysvětlení pojmů

Master kód umožňuje nastavovat / odstavovat libovolnou skupinu systému libovolným způsobem, měnit, mazat a zadávat ostatní uživatelské kódy. Pouze master kód umožňuje měnit nebo mazat uživatelské kódy přiřazené oběma skupinám.

Master kód 1 je natrvalo přiřazen skupině 1 a umožňuje měnit, přidávat a mazat uživatelské kódy přiřazené právě skupině 1.

Master kód 2 je natrvalo přiřazen skupině 2 a umožňuje měnit, přidávat a mazat uživatelské kódy přiřazené právě skupině 2. [10]

6.6.3 Programovací sekce uživatelských kódů

V programovací sekci uživatelských kódů zvolíme, který uživatelský kód nebo master kód se bude měnit.

Sekce	Uživatelský kód
[001]	Uživatelský kód 001 = Systémový master kód
[002]	Uživatelský kód 002 = Master kód 1
[003]	Uživatelský kód 003 = Master kód 2
[004] až [047]	Uživatelský kód 004 až 047
[048]	Uživatelský kód 048 nebo nátlakový kód

Obrázek 28. Programování uživatelských kódů u ústředny Spectra [10]

6.7 Programování parametrů uživatelských kódů

Parametry uživatelských kódů se programují pomocí postupu popsaného v kapitole 6.3. Programovací sekce se zvolí 302-348 v závislosti na uživatelském kódu, který chceme nastavit. Následuje nastavení parametrů, které je popsáno v kapitole 6.7.2.

6.7.1 Programovací sekce 302-348

Programovací sekce 302-348 určí, jestli se budou programovat parametry master kódu nebo uživatelských kódů a o který kód půjde. Viz obr. 29.

Sekce #		Parametry kódů	Sekce #		Parametry kódů
[302]	Master kód 1	1 2 3 4 5 6 7 8	[325]	Uživatelský kód 025	1 2 3 4 5 6 7 8
[303]	Master kód 2	1 2 3 4 5 6 7 8	[326]	Uživatelský kód 026	1 2 3 4 5 6 7 8
[304]	Uživatelský kód 004	1 2 3 4 5 6 7 8	[327]	Uživatelský kód 027	1 2 3 4 5 6 7 8
[305]	Uživatelský kód 005	1 2 3 4 5 6 7 8	[328]	Uživatelský kód 028	1 2 3 4 5 6 7 8
[306]	Uživatelský kód 006	1 2 3 4 5 6 7 8	[329]	Uživatelský kód 029	1 2 3 4 5 6 7 8
[307]	Uživatelský kód 007	1 2 3 4 5 6 7 8	[330]	Uživatelský kód 030	1 2 3 4 5 6 7 8
[308]	Uživatelský kód 008	1 2 3 4 5 6 7 8	[331]	Uživatelský kód 031	1 2 3 4 5 6 7 8
[309]	Uživatelský kód 009	1 2 3 4 5 6 7 8	[332]	Uživatelský kód 032	1 2 3 4 5 6 7 8
[310]	Uživatelský kód 010	1 2 3 4 5 6 7 8	[333]	Uživatelský kód 033	1 2 3 4 5 6 7 8
[311]	Uživatelský kód 011	1 2 3 4 5 6 7 8	[334]	Uživatelský kód 034	1 2 3 4 5 6 7 8
[312]	Uživatelský kód 012	1 2 3 4 5 6 7 8	[335]	Uživatelský kód 035	1 2 3 4 5 6 7 8
[313]	Uživatelský kód 013	1 2 3 4 5 6 7 8	[336]	Uživatelský kód 036	1 2 3 4 5 6 7 8
[314]	Uživatelský kód 014	1 2 3 4 5 6 7 8	[337]	Uživatelský kód 037	1 2 3 4 5 6 7 8
[315]	Uživatelský kód 015	1 2 3 4 5 6 7 8	[338]	Uživatelský kód 038	1 2 3 4 5 6 7 8
[316]	Uživatelský kód 016	1 2 3 4 5 6 7 8	[339]	Uživatelský kód 039	1 2 3 4 5 6 7 8
[317]	Uživatelský kód 017	1 2 3 4 5 6 7 8	[340]	Uživatelský kód 040	1 2 3 4 5 6 7 8
[308]	Uživatelský kód 018	1 2 3 4 5 6 7 8	[341]	Uživatelský kód 041	1 2 3 4 5 6 7 8
[319]	Uživatelský kód 019	1 2 3 4 5 6 7 8	[342]	Uživatelský kód 042	1 2 3 4 5 6 7 8
[320]	Uživatelský kód 020	1 2 3 4 5 6 7 8	[343]	Uživatelský kód 043	1 2 3 4 5 6 7 8
[321]	Uživatelský kód 021	1 2 3 4 5 6 7 8	[344]	Uživatelský kód 044	1 2 3 4 5 6 7 8
[322]	Uživatelský kód 022	1 2 3 4 5 6 7 8	[345]	Uživatelský kód 045	1 2 3 4 5 6 7 8
[323]	Uživatelský kód 023	1 2 3 4 5 6 7 8	[346]	Uživatelský kód 046	1 2 3 4 5 6 7 8
[324]	Uživatelský kód 024	1 2 3 4 5 6 7 8	[347]	Uživatelský kód 047	1 2 3 4 5 6 7 8
			[348]	Uživatelský kód 048	1 2 3 4 5 6 7 8

Obrázek 29. Programovací sekce 302-348 u ústředny Spectra [10]

6.7.2 Nastavení parametrů kódu

Parametry kódu se nastaví zmáčknutím jednotlivých čísel. Aktivace je signalizována rozsvícením.

[1] svítí = ovládání skupiny 1

[2] svítí = ovládání skupiny 2

[3] svítí = povolení přemostění zón

[4] svítí = nastavení STAY

[5] svítí = nucené nastavení (FORCE)

[6] svítí = pouze nastavení

[7] svítí = pouze aktivace PGM

[8] svítí = nepoužito [10]

V případě zadání čísla 6 lze systém pouze zastřežit. Povolení přemostění zón, nastavení STAY a nucené nastavení (FORCE) bude vysvětleno v následující kapitole.

6.8 Programování dalších funkcí

6.8.1 Dělení systému

Pomocí postupu, který je zmíněn v kapitole 6.3 je nejprve nutné povolit dělení systému v sekci 127 číslicí 1. Dále je třeba přidělit skupinu jednotlivým zónám a uživatelským kódům. Pokud systém rozdělíme, lze přiřadit každou zónu, každého uživatele jedné, druhé nebo oběma skupinám. Jestliže systém není dělen, jsou všechny uživatelské kódy a všechny parametry vztažené ke skupině 1.

6.8.2 Odchodové zpoždění

Odchodové zpoždění první skupiny lze nastavit pomocí postupu v kapitole 6.3 v sekci 071 třemi číslicemi, které zadají počet sekund, kdy nebude systém reagovat na narušení zóny. Odchodové zpoždění druhé skupiny lze zadat stejným způsobem v sekci 072.

6.8.3 Ruční přemostění (BYPASS)

První je nutné povolit přemostění jak v zóně i v uživatelských parametrech.

Tato funkce umožňuje úplné vynechání vybraných zón, které trvá už do dalšího nastavení. Tuto funkci nelze aplikovat na požární zóny, lze ji aktivovat jednou klávesou.

Postup při přemostění zóny:

1. Stiskneme tlačítko [BYP]

2. Zadáme platný [UŽVATELKSKÝ KÓD]

3. Vybereme zónu(y) pro přemostění

4. Po zadání potvrdíme výběr klávesou [ENTER].

6.8.4 Částečné nastavení (STAY)

Tento způsob se využívá, pohybují – li se i po nastavení v části objektu lidé. Tento způsob lze například použít pro noční zabezpečení dveří a oken.

Postup pro nastavení funkce STAY:

1. Všechny zóny v požadované části objektu musí být uzavřeny.

2. Stiskneme tlačítko [STAY]

3. Zadáme platný [UŽVATELKSKÝ KÓD]. [10]

Po zadání budou zastřeženy pouze zóny, které přísluší danému uživatelskému kódu a zároveň mají povolenou funkci STAY.

Pro správnou funkčnost musí mít i uživatelský kód povolenou funkci STAY.

6.8.5 Nucené nastavení (FORCE)

Tímto způsobem lze nastavit narychlo systém bez nutnosti vyčkat na uzavření všech zón. Pokud je u smyčky povolen parametr nuceně (FORCE), ústředna ignoruje otevření této zóny v okamžiku nastavování. Pokud po uplynutí této doby dojde k uklidnění zóny, ústředna tuto zóny uvažuje jako aktivní a dojde–li k poplachu (opětovnému narušení), bude ústředna reagovat klasicky na poplachovou událost. Pro správné fungování musí být nastavena zóna na nucenou zónu a uživatelský kód musí mít povolenou funkci FORCE. Nucené nastavení se provede pomocí tlačítka FORCE a následně zadáme uživatelský kód.

6.8.6 Změna instalačního a master kódu

Postup je opět zmíněný v kapitole 6.3. Pro instalační kód se použije sekce 281 a pro master kód sekce 301, poté lze zadat čtyřmístné číslo, které se uloží jako nový instalační nebo master kód.

6.8.7 Nastavení příchodového času

Pro příchodový čas je nutné nastavit zónu na vstupní zpoždění a příchodový čas se nastaví pomocí postupu v kapitole 6.3 pomocí sekce 069.

7 TESTOVÁNÍ BEZPEČNOSTI DRÁTOVÝCH ÚSTŘEDEN TYPU NO A NC

Celý postup testování bezpečnosti drátových ústředen včetně rozborů přiložených videí a možnosti opatření pro zvýšení bezpečnosti drátových ústředen je popsán v Příloze III: Testování bezpečnosti drátových ústředen.

ZÁVĚR

Cílem bakalářské práce bylo nejen přiblížit účel jednotlivých částí ústředny, ale především podrobně popsat způsoby ochrany analogových drátových ústředen před sabotáží. Nechybí zde i popis změn v normě ČSN EN 50131, která se zabývá poplachovými zabezpečovacími systémy včetně podrobného popisu požadavků aktuální normy ČSN EN 50131-1/A1 z roku 2009 na ochranu proti sabotáži v závislosti na stupni zabezpečení. Zapojení smyček u analogových drátových ústředen je zde rozděleno na NO (normally opened) a NC (normally closed). Dále jsou zde popsány jednotlivé možné způsoby zapojení včetně výhod a nedostatků jednotlivých zapojení.

Praktická část obsahuje popis a realizaci testování bezpečnosti analogových drátových ústředen. Je v ní uveden podrobný popis způsobu programování ústředny Spectra, která byla použita pro testování. Dále jsou představeny základní parametry ústředny včetně zobrazení poruch, následuje podrobný popis testování ústředny. Vše je podrobně zdokumentováno na videu „V1“. Práce obsahuje také video „V2“ a „V3“, kde je znázorněna účinnost celého postupu. V další části je popsán rozbor získaných výsledků, požadavky normy ČSN EN 50131 na odolnost analogových ústředen proti celému postupu a podmínky, za kterých je možné v praxi uskutečnit zmíněný postup. Nakonec jsou navrženy možnosti opatření pro zvýšení bezpečnosti drátových ústředen, čímž je možné nejen zabránit finančním ztrátám, které by mohly vzniknout v případě ponechání současných požadavků norem na zabezpečení drátových ústředen, ale také ochránit život a zdraví. Život a zdraví může poplachová zabezpečovací signalizace chránit pomocí spuštění poplachové signalizace, která může přimět narušitele utéct. Tím lze zabránit nebezpečnému střetnutí majitele objektu s narušitelem.

Výsledky dosažené v bakalářské práci vedly k velmi závažnému zjištění, které bylo podrobně popsáno v praktické části. Pomocí zmíněných možností opatření lze zlepšit úroveň zabezpečení majetku. Vzhledem k současné narůstající kriminalitě je nutné uvědomit si zmíněné nebezpečí a chránit sebe a svůj majetek pomocí kvalitních a spolehlivých poplachových zabezpečovacích systémů.

ZÁVĚR V ANGLIČTINĚ

The objective of this work was to describe functions of the main part of security central and give ways to protect against sabotage of the analog centrals. There are also mentioned changes of the norm ČSN EN 50131-1 which deals with alarm security systems including current norm ČSN EN 50131-1/A1 from 2009 for protection against sabotage, depending on security level. Wired zones for analog wired centrals are separated up into NO (normally opened) and NC (normally closed). Moreover, methods of wiring with advantages and disadvantages are described.

Practical part deals with the safety testing of the analog central. There is a detailed description of the programming method of security central Spectra, which was used for testing. Then, there are basic parameters, including a failures indication and detailed description of the security central testing. Everything is documented on the video „V1". The work includes also the video "V2" and "V3", which show the effectiveness of the whole procedure. In the next section, there is described a retrieved results analysis, norm ČSN EN 50131 requirements for analog security central resistence to the whole process and the conditions under which it is possible in practice to implement the mentioned procedure. Finally, there are action possibilities to improve a wired security central safety. This is possibility to prevent financial losses that might arise in case of letting current norm requirements for the security central, but also to protect life and health. Life and health the alarm security signalization may protect the execution of signaling, which may cause the intruder to escape. This can prevent a dangerous confrontation the property owner with the intruder.

The result of this work lead to a very serious finding, which is mentioned in the practical part. Due to mentioned possibilities at the end of the practical part, the level of security of property may be improved. With regard to the current rising crime it is important to be aware of that danger and protect himself and his property by the help of alarm security systems.

SEZNAM POUŽITÉ LITERATURY

[1] *CSN EN 50131-1 ed. 2*. Praha : Český normalizační institut, 2007. 40 s.

[2] JUDR. ČERNÝ, Josef; ING. IVANKA, Ján. *Systemizace bezpečnostního průmyslu I*. Zlín : Univerzita Tomáše Bati, 2006. 135 s.

[3] JAN, Uhlář. *Technická ochrana objektu II*. Praha : Policejní akademie ČR, 2001. 224 s.

[4] VOTRUBA, Zdeněk. *Historie zabezpečovacích systému* [online]. 2009 [cit. 2010-05-09]. Terminologie a funkce prvků EZS. Dostupné z WWW: <http://webcache.googleusercontent.com/search?q=cache:n94TQ_w_xQgJ:skola.spectator.cz/3_SEMESTR/Firemni%2520Prezentace/Terminologie.pps+koncentratorove+ustredny&cd=19&hl=cs&ct=clnk&gl=cz>.

[5] *Instalační manuál ústředny Galaxy G3* [online]. [s.l.] : Honeywell Security, 2000 [cit. 2010-04-22]. Dostupné z WWW: <http://www.dvisystems.co.uk/sitebuildercontent/sitebuilderfiles/galaxy_g3_installation_manual.pdf>.

[6] STANISLAV, Křeček. *Příručka zabezpečovací techniky*. Blatná : Blatenská tiskárna s.r.o, 2002. 350 s.

[7] *CSN EN 50131-1/A1*. Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010. 12 s.

[8] *ASITA spol. s r.o.* [online]. 2010 [cit. 2010-04-30]. Rozvodné krabice. Dostupné z WWW: <http://asita.trade.cz/rozvodne-krabice>.

[9] ING. KINDL, Jiří. *Projektování bezpečnostních systémů I*. Zlín : Univerzita Tomáše Bati, 2007. 133 s.

[10] *Instalační manuál ústředny Spectra*. [s.l.] : PARADOX SECURITY SYSTEMS, 2003. 52 s.

[11] *GUTA Servis - zabezpečovací systémy* [online]. 2009 [cit. 2010-05-11]. Elektronické zabezpečovací systémy. Dostupné z WWW: <http://www.guta-servis.cz/elektronicke-zabezpecovaci-systemy-ezs.php#signalizace>.

[12] *Lotter* [online]. 2009 [cit. 2010-05-11]. Electronická ostraha objektů . Dostupné z WWW:

<http://www.loter.eu/index.php?option=com_content&view=article&id=47&Itemid=59>.

[13] *Emos* [online]. 2007 [cit. 2010-05-11]. Zabezpečovací systémy. Dostupné z WWW: <http://www.emos.cz/montaze-a-servis/zabezpecovaci-systemy/>.

[14] *Instalační manuál Galaxy* [online]. Motherwell : Honeywell Security, 2004 [cit. 2010-05-11]. Dostupné z WWW: <http://www.dvisystems.co.uk/sitebuildercontent/sitebuilderfiles/galaxy_g3_installation_manual.pdf>.

[15] *Elektronické zabezpečovací systémy* [online]. 2008 [cit. 2010-05-11]. Elektro-Mahdl. Dostupné z WWW: <http://www.elektro-mahl.cz/dokumenty/index.php>.

[16] *DSC Power* [online]. 2007 [cit. 2010-05-11]. ALARMY s.r.o. Dostupné z WWW: <http://www.alarmysro.sk/index.php?page=3667>.

[17] *Zabezpečovací systémy* [online]. 2009 [cit. 2010-05-11]. MH-elektro. Dostupné z WWW: <http://www.mh-elektro.cz/>.

[18] *EZS - elektronické zabezpečovací systémy* [online]. 2008 [cit. 2010-05-11]. ALARMTEC. Dostupné z WWW: <http://www.alarmtec.cz/ezs-elektronicke-zabezpecovaci-systemy.html>.

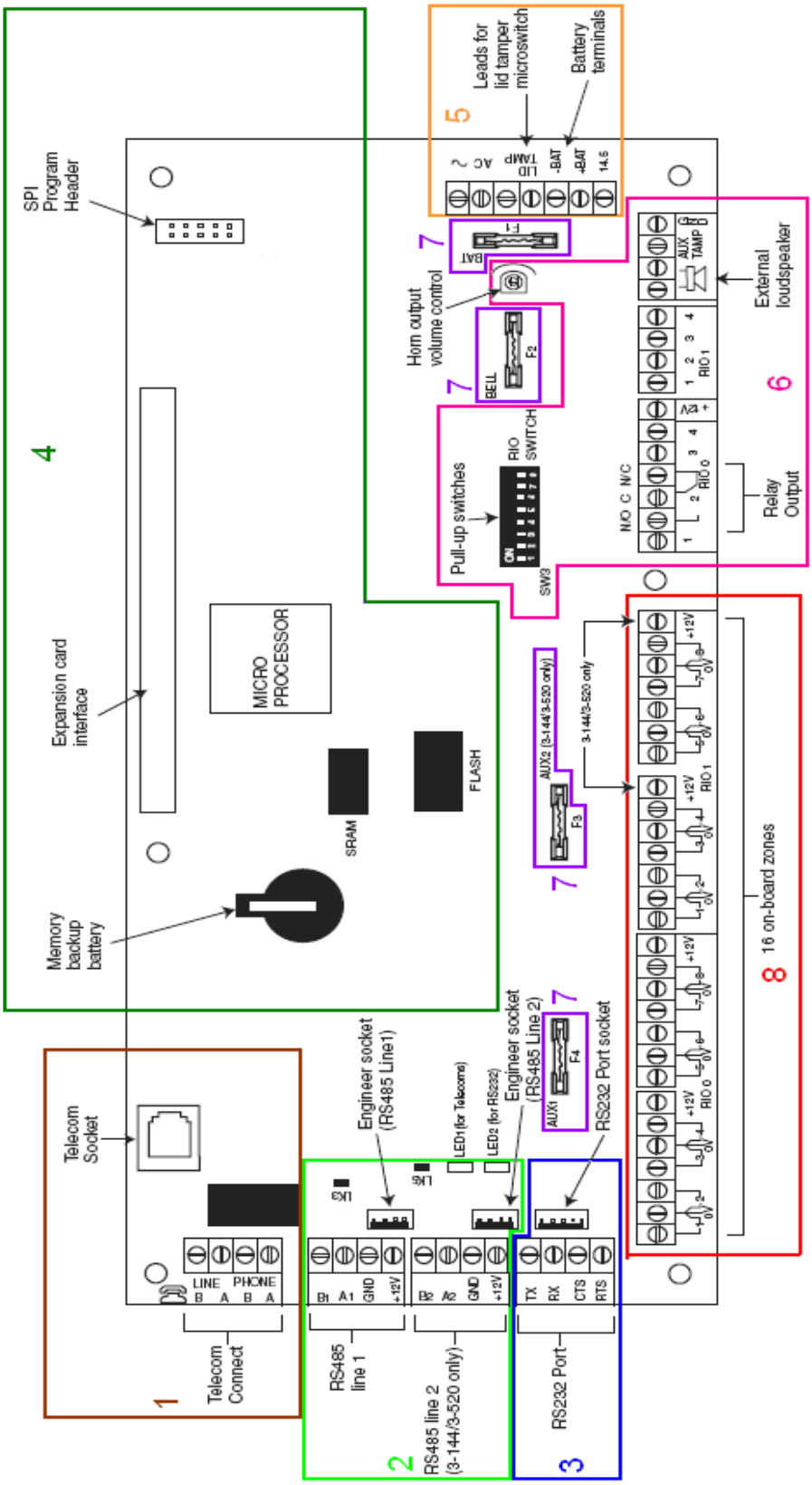
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

EZS	Elektronická zabezpečovací signalizace
PZS	Poplachové zabezpečovací systémy
PCO	Pult centralizované ochrany
IAS	Intruder Alarm System
HAS	Hold-up Alarm System
PTS	Poplachové tísňové systémy
I&HAS	Intruder and Hold-up Alarm System
NO	Normally opened
NC	Normally closed
PZTS	Poplachové zabezpečovací a tísňové systémy
PGM	Programovatelný výstup
RIO	Remote Input Ouput
GSM	Global system module
SMS	Short message
mA	Miliampér-jednotka elektrického proudu
V	Volt-jednotka napětí
Ω	Ohm-jednotka elektrického odporu

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: ZÁKLADNÍ DESKA ÚSTŘEDNY GALAXY G3



PŘÍLOHA P II: POJISTKY ÚSTŘEDNY GALAXY G3