Technická ochrana objektů v podmínkách Policie České republiky

Marek Musil

Bakalářská práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Marek Musil**
Osobní číslo:	**L20096**
Studijní program:	**B1032A020002 Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Technická ochrana objektů v podmínkách Policie České republiky**

Zásady pro vypracování

1. Zpracujte základní teoretická východiska oblasti poplachových zabezpečovacích a tísňových systémů.
2. Vyberte objekt a zhodnoťte jeho současný stav.
3. Navrhněte možná řešení pro objekt z hlediska elektronického zabezpečení.

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

Seznam doporučené literatury:

1. BURDA, Karel. *Základy elektronických zabezpečovacích systémů*. Brno: Akademické nakladatelství CERM, 2017. ISBN 978-80-7204-967-7.
2. KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-80-260-7115-0
3. MAUGHAN, Joel. *Home Security Systems: Home Security Tips Revealed* [online]. Lulu Press [cit. 2022-11-15], 2016. ISBN 9781329981973. Dostupné z: https://play.google.com/books/reader?id=rUPVCwAAQBAJ&pg=GBS.PT4&hl=en_US

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Martin Ficek**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. prosince 2022**
Termín odevzdání bakalářské práce: **5. května 2023**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2022

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- 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;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- 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);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- 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 obsahově totožné.

V Uherském Hradišti, dne: 5. 5. 2023

Jméno a příjmení studenta: Marek Musil

.....
podpis studenta

ABSTRAKT

Bakalářská práce se zabývá návrhem zabezpečení budovy Policie ČR. Teoretická část práce je zaměřena na poplachové tísňové a zabezpečovací systémy z obecného hlediska, složení a použití dle prostředí a třídy zabezpečení. V praktické části je provedena analýza současného stavu objektu, s důrazem na bezpečnost a složitost, a to jak z pohledu uživatele, tak technika. Provedený návrh zabezpečení objektu policie byl proveden tak, aby byl jednotný, komplexní a uživatelsky přívětiví v souladu s bezpečnostními normami.

Klíčová slova: Poplachový zabezpečovací a tísňový systém, dohledové a poplachové přijímací centrum, technická ochrana, zabezpečení objektu, detektor, ústředna

ABSTRACT

The bachelor thesis deals with the design of the security of the building of the Police of the Czech Republic. The theoretical part of the thesis is focused on emergency alarm and security systems from a general and legal point of view. In the practical part, an analysis of the current state of the building is carried out, with emphasis on security and complexity, both from the user's and technician's point of view. The design of the security of the PCR facility has been carried out to be uniform, comprehensive and user-friendly in accordance with security standards.

Keywords: Intrusion and Hold-Up Alarm Systems, Monitoring alarm and receiving centre, Technical protection, Facility security, Detector, Control panel

Nejdříve bych na tomto místě velmi rád poděkoval vedoucímu bakalářské práce panu Ing. Martinu Fickovi, Ph.D. za trpělivost, inspiraci, podporu a jeho pomoc při vedení během tvorby této bakalářské práce.

Dále bych poděkoval své rodině, manželce, ale také zaměstnavateli za jejich trpělivost a podporu během celého studia.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

V různém pojetí lidé „bezpečností systémy“ využívají od nepaměti. Logicky to však nebyly vždy technické vymoženosti dnešní doby. V dřívějších dobách, kdy lidé potřebovali chránit zejména své zdraví, život a obydlí se využívalo zejména materiálových prostředků, např. otevřený oheň, zákopy, jeskyně apod. nebo osobní ochrany-stráže. Jak šel čas, tak se ochrana vyvíjela, zdokonalovala a byly vynalézány různé oplocení, bezpečnostní dveře, až po dnešní technicky vyspělé bezpečnostní systémy neboli „Poplachové bezpečnostní a záznamové zařízení“.

S lidských vývojem se rovněž rozšiřuje množství statků, které je potřeba chránit. Mimo základní objekty zájmu jako jsou samozřejmě život, zdraví a majetek, se do oblasti zabezpečení dostávají informace, cennosti, památky apod. V sektoru policie, ale také např. armády, celní správy atd. hrají informace a jejich ochrana důležitou roli. V budovách těchto institucí se mnohdy nacházejí informace, které podléhají utajení, a tak je nezbytné tyto informace chránit před únikem. V rámci Policie ČR se samozřejmě takové informace nacházejí ve většině budov, a proto mají tyto budovy svůj specificky daný režim a zabezpečení. Praktická část práce se zaměří na jednu z takových budov, kde se tyto informace nacházejí.

Bakalářská práce je zaměřena na návrh zabezpečení objektu Policie ČR. Budova, která je objektem zájmu práce, je zabezpečena staršími technologiemi a bezpečnostní systém je „roztříštěný“ na více malých ústředen, případně přenosových zařízení s menším množství prvků (detektory, magnetické kontakty …).

Cílem práce je navrhnout Poplachový zabezpečovací a tísňový systém pro vybraný objekt Policie ČR. Za účelem vytvoření kompletního zabezpečení a sjednocení technologií do jednoho systému, který bude implementován do jediné ústředny.

I. TEORETICKÁ ČÁST

1 POPLACHOVÉ ZABEZPEČOVACÍ A TÍSŇOVÉ SYSTÉMY

Poplachový zabezpečovací a tísňový systém (dále jen „PZTS“) doplňuje systém zabezpečení jako jsou například bezpečnostní dveře, okna, ploty apod. Prvořadou myšlenkou a úlohou PZTS je zajištění bezpečnosti osob a majetku. Bezpečnostní elektronický systém sloužící zejména k detekci a následné signalizaci narušení chráněného prostoru např. pomocí detektoru pohybu, magnetického kontaktu atd. Moderní bezpečnostní systémy jsou však navrženy tak, aby byly schopny případnou detekci narušení následně vyhodnotit a dle naprogramování zareagovat aktivně, například zamlžovacím prvkem, zamknutím dveří, nebo spuštěním hasícího systému a předejít tak většímu požáru. Jako většina elektronických zařízení i PZTS podléhá zákonům a normám ČR.

Statistiky ukazují, že 60 % domů zabezpečených poplachovým systémem s alarmovou detekcí je neúspěšných v případě napadení. Z toho plyne, že v řadě případů je bezpečnostní systém užitečný. Pachatelé si při výběru svého cíle, vybírají ty objekty, které jsou snáze přístupné a co nejméně rizikové, tak aby nebyli přistiženi. Co se týče zabezpečení domů, je stěžejní provést bezpečnostní posouzení objektu. V tomto zahrnout kritická místa jako dveře, okna, ale také třeba venkovní osvětlení, oplocení, přístupové cesty apod. Rovněž je nasnadě zmonitorovat situaci v dané oblasti a kriminalitu jaká se zde vyskytuje. Dle bezpečnostního posouzení pak navrhnout zabezpečovací systém pro konkrétní budovu. V současné době již existují systémy, které jsou snadné svou instalací a nepotřebují ani rozsáhle stavební úpravy zapříčiněné elektroinstalací. Dají se například využít bezdrátové systémy. Co se týká bezpečnosti jako takové, není vždy nutno hned investovat velké finanční prostředky do nákladných komplexních systémů s přenosem na dohledové přijímací a poplachové centrum (dále jen „DPPC“) se zásahovou službou. Někdy postačí reálné zhodnocení a vybavení domu například venkovním osvětlením s detekcí pohybu, kamerou atd., již takové prvotní visuální vybavení může pachatele odradit od případného vloupání. (Maughan, 2016)

1.1 Právní ukotvení problematiky

Právní ukotvení problematiky poplachových zebezpečovacích a tísňových systémů vychází zejména z právních norem. V České republice doporučuje normy pro PZTS Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ).

„Postavení ČSN podle zákona č. 22/1997 Sb., o technických požadavcích je dobrovolné/nezávazné, avšak v řadě právních předpisů se setkáváme s odkazy, kde naplnění

právního požadavku je vázáno na splnění požadavků konkrétní technické normy. Povinnost postupovat při určité činnosti v souladu s ČSN vzniká především na základě ustanovení právního předpisu.“ (Závaznost norem, c2020)

ČSN EN 50131-1 ed. 2 Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky. Obsahem normy jsou požadavky na jednotlivé detektory výstražná zařízení, napájecí zdroje aj.

ČSN EN 50131-2-2 ED.2 (334591) Poplachové zabezpečovací a tísňové systémy. Tato norma se zabývá pasivními infračervenými detektory. Jsou zde stanoveny požadavky na provoz, funkci, odolnost aj.

ČSN EN 50131-3 (334591) Poplachové zabezpečovací a tísňové systémy. Norma 50131 část 3 je věnována zejména ústřednám, ale také jsou zde uvedeny detektory, například infračervené/mikrovlnné, detektory rozbití skla, magnetické kontakty a další zařízení.

ČSN CLC/TS 50131-7 Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace

ČSN EN 50131-6 ED.3 (334591) Poplachové zabezpečovací a tísňové systémy – Část 6: Napájecí zdroje

TNI 33 4591-1: část 1 návrh systému PZTS

Norma pro návrh systému, bezpečnostní posouzení, obsah projektové dokumentace, značky a zkratky pro projektování, vzorové zabezpečení objektu.

TNI 33 4591-2: část 2 montáž PZTS

Norma pro montáž systému – ústředny, napájecí zdroj, ovládací zařízení, detektory, signalizační, zařízení, kabeláž.

TNI 33 4591-3: část 3 uvedení PZTS do provozu a jeho následný provoz, údržba a servis prohlídka systému, funkční zkouška, revize elektrického zařízení, proškolení obsluhy, zkušební provoz, pravidelná kontrola a údržba (Technické normy, c1998-2023)

Požadavky na PZTS byly dříve pro konkrétní typy systémů stanoveny v normách EN 50130-50137 (Kyncl, 2014), v současné době je to norma ČSN EN 50131, která má 13 částí.

1.2 Předmět zájmu

Poplachové zabezpečovací a tísňové systémy jsou užitečné a doceněné pouze tam, kde jsou užity správným způsobem a za daným účelem. Z toho důvodu je důležité mít stanovený objekt nebo předmět zájmu, který chceme mít pod ochranou. Mezi takové hodnoty můžeme zařadit informace, objekty (předměty), budovy nebo celé areály. Následně dle analýzy

a vyhodnocení daného problému je možno navrhnout specifické řešení bezpečnostního systému.

Informace

Informace pochází z latinského slova in-formatio což v předkladu znamená „utváření, ztvárnění“. Je to mnohoznačný a velmi obsáhlý pojem, který může být využit mnoho způsoby. Informace může být například myšlenka, znalost, zkušenost, ale také taková informace, která bude užitečná až v budoucnu. Z pohledu technologického zabezpečení informace je možno zabezpečit pouze takové informace, které jsou zaznamenány na papír, v podobě dat na mediálních nosičích, počítači, cloudovém úložišti apod.

V rámci utajení existují čtyři stupně utajení informace:

a) vyhrazené,

b) důvěrné,

c) tajné,

d) přísně tajné. (ČESKO, 2015)

Objekt

Z pohledu elektronického zabezpečení je předmětným zájmem ochrany právě objekt, ať už se jedná o osobu, věc, budovu nebo dokonce areál podniku. Pod pojmem věc si můžeme představit drobný předmět, trezor, ale také třeba osobní automobil, automobil na převoz finančních prostředků, drahých kovů, cenností apod.

Bezpečnostními technologiemi je možno zabezpečit a automatizovat prostory areálu podniku. Příkladem může být například kamera umístěná u vjezdové závory. Při vjezdu vozidla kamera rozpozná registrační značku zavedenou v systému a závora se následně otevře. Areál je možno dále zabezpečit např. kamerami s detekcí pohybu a upozornit tak ostrahu objektu. Samotný objekt a věci je již možno zajistit detektory pohybu, magnetickými detektory apod. Právě těmito detektory se práce zabývá a jejich detailní popis je uveden v následujících kapitolách.

1.3 Bezpečnostní posouzení

Základem každého technického zabezpečovacího systému je bezpečnostní posouzení daného objektu. V tomto jsou v ideálním případně zohledněny všechny možné cesty napadení objektu, případná trasa narušitele (útočníka). Dále možná rizika spojená s předmětným objektem, jako jsou slabá místa budovy, perimetru tzv. kritická místa.

V takovém posudku nesmí chybět zhodnocení a zařazení objektu dle příslušné bezpečnostní kategorie, pro případnou instalaci konkrétních prvků a následný návrh technického řešení zabezpečení. (Kyncl, 2014)

V bezpečnostním posouzení musí být rovněž stanovený cíl, návrh, kde by mělo být jasně vytyčeno, co konkrétně je předmětem zájmu. Stanovit jasně dané priority a požadavky na bezpečnostní systém. Např. zda je požadována instalace pouze elektronického zabezpečovacího systému, nebo je cílem vytvořit komplexní systém s kontrolou vstupu, případně docházkovým systémem apod.

1.4 Základní terminologie

V literaturách se vyskytuje mnoho názvů a názvosloví, mnohdy je daná součást bezpečnostního systému označována různými výrazy, z toho důvodu a také pro potřeby porozumění práce, je níže uveden krátký seznam důležitých výrazů v oblasti poplachových a tísňových systémů a uveden stručný popis.

Poplachový zabezpečovací a tísňový systém

Jedná se o soubor zařízení a programového vybavení. Tento systém je schopen odesílat a přijímat data mezi objektem a uživatelem, případně DPPC. Bývá označován rovněž jako EZS (elektronický zabezpečovací systém) nebo PZS (poplachový zabezpečovací systém). V anglické literatuře se můžeme setkat se zkratkou I&HAS, což jsou první písmena z anglického Intrusion and Hold-Up Alarm Systems. V rámci Policie ČR je využíváno zkratky PZTS.

Dle Burdy lze PZS definovat jako elektronický systém, který je určený k detekování a následnému odeslání signálu při vzniku nežádoucího incidentu v oblasti zájmu. Touto oblastí je míněn kontrolovaný majetek, který je systémem zabezpečen. (Burda, 2017)

Dohledové poplachové a přijímací centrum

Jedná se o systém vzdáleného dohledu nad objektem, který je opatřen zabezpečovacím systémem. Obsluha DPPC je osoba dohlížející na počítač, kde běží program, do kterého jsou posílány jednotlivé poplachové, ale i technické události jako např. vybitá baterie. U policie je takovou osobou operační důstojník integrovaného operačního střediska (dále jen „IOS“). V tomto programu může být zaimplementováno velké množství zabezpečených objektů. Při příchodu události operátor DPPC následně reaguje a případně koordinuje postup vyslaných hlídek. V praxi to znamená, že každé krajské území v gesci Policie ČR má své integrované operační středisko, v jehož rámci je vybudováno DPPC.

Detektor

Koncový prvek v systému, který vyhodnocuje fyzikální děje a následně zasílá do ústředny událost, která vyhlásí poplach. Typicky se jedná o prostorové čidlo, které reaguje na pohyb pachatele, ale také např. magnetické kontakty, otřesová čidla apod.

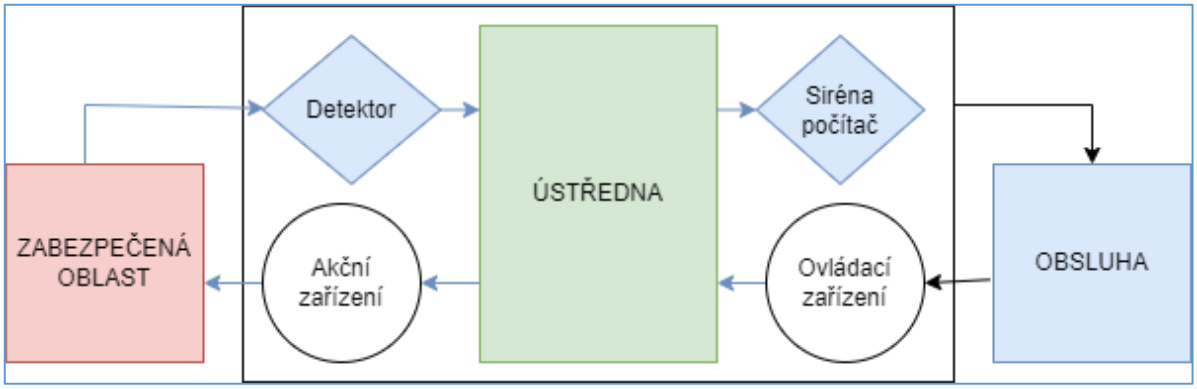
Elektronická kontrola vstupu

Elektronickou kontrolu vstupu (dále jen „EKV“) můžeme definovat jako elektronický systém, určený k automatizaci a kontrole přístupů do předmětné oblasti. Systém spravuje tzv. autorita, jedná se o osobu, která má práva k tomu určit kdo a kam může mít přistup. Systém umožňujíce regulaci pohybu osob a také ztížení postupu útočníka. Může se jednat o vícevrstvou ochranu jako vstup přes bránu v oplocení, vstup do budovy a vstupy např. do jednotlivých kanceláři atd. (Burda, 2017)

2 ARCHITEKTURA ZABEZPEČNOSTNÍCH SYSTÉMŮ

Jako každý systém a stavba má svou vlastní architekturu ani u bezpečnostních systémů tomu není jinak. K tomu, aby mohl zabezpečovací systém plně a spolehlivě fungovat je nutné mít veškeré zařízení a komponenty v PZTS správně nainstalovány a připojeny. Každé elektronické zařízení v systému má svůj význam, místo a požadavky. Tyto pokyny musí být splněny jinak by mohlo dojít k situaci, kdy systém přestane fungovat, případně vykazovat závady a poruchy, které se následně těžce diagnostikují. Následné opravy, kupříkladu v opravení kabelového vedení a spojů, bývají časově a technicky náročné. Proto je velmi důležité již při plánovaní PZTS, vše rozvrhnout tak, aby montáž a zapojení byla smysluplná, technicky správná a pokud možné nekomplikovaná, „jednoduchá“.

Burda ve své knize z roku 2017 popisuje PZTS na následujícím obrázku (obr. č. 1), kdy signál z detektoru (čidlo, magnetický kontakt) přenosem do ústředny spustí hlášení o vzniku incidentu. Následně skrze informační zařízení (počítač, siréna) informuje obsluhu, která následně provede potřebná opatření. Například kontrolou ovládacího zařízení. Moderní bezpečnostní systémy mohou mít i tzv. akční zařízení, které jsou spuštěny ústřednou, za předem stanovených podmínek. Takovými zařízeními mohou být například zamlžovací zařízení.



Obrázek 1: Schéma PZTS, vlastní zpracování (Burda, 2017)

2.1 Ústředny a jejich dělení

Ústředna v zabezpečovacím systému je jakýmsi „mozkem“ celé soustavy elektronických komponent a prvků. Toto elektronické zařízení je v dnešní době charakterizováno jako řídící počítač, ke kterému jsou připojeny periferní zařízení. Toto propojení může být provedeno několika způsoby a sice metalicky, radiově nebo bezdrátově. Z koncových zařízení je do ústředny přes předem danou přenosovou cestu vyslán signál, který je následně ústřednou

zpracován a vyhodnocen. Jako výsledek takového procesu je z ústředny vyslána informace např. směrem k siréně, ta následně spustí akustický poplach a upozorní uživatele o narušení střeženého prostoru.

V současné době jsou ústředny již opravdu počítače a mají mnoho funkcí, avšak tou prioritní a prvotní funkcí je stále bezpečnost. Průmyslové počítače lze programovat a v softwarové nadstavbě vytvářet nejrůznější funkce. K těm nejdůležitějších jistě patří rozdělení zastřeženého objektu na podsystémy (podobjekty), kdy tyto následně lze zastřežit a odstřežit jednotlivě. Správné rozvržení a nastavení podsystémů má v rámci ochrany své opodstatnění a využití. V rámci Policie ČR např. zbrojní sklad, tento je zabezpečený permanentně a odstřeží se jen v případě, kdy je zapotřebí. Oproti tomu, prostor oddělení policie, kde je v průběhu pracovní doby pohyb zaměstnanců, je odstřežen.

Z toho vyplývá, že nejdůležitějšími stavy, ve kterých se může ústředna, nebo daný podsystém nacházet je „Vzato pod ochranu“ (zastřeženo) a „vyjmuto z ochrany“ (odstřeženo). V případě, kdy je se v prostoru, který je vzat pod ochranu nainstalováno prostorové čidlo a někdo by do tohoto prostoru vstoupil, je vyslán z detektoru pohybu do ústředny signál o narušení a následně se spustí poplach na DPPC PČR. Naopak v situaci, kdy prostor zastřežený není se poplach nevyhlašuje. Při programování ústředny lze nastavit, aby konkrétní koncový prvek, např. detektor požáru vyhlásil poplach i v případě, že není objekt zastřežen. Další situací, kdy je vyhlášen poplach je přerušení kontaktu tamperu (ochranného kontaktu), to znamená, že dojde k „poruše“ na zařízení, lépe řečeno k sabotáži. Vyhlášení tohoto stavu tedy nastane například v případě, kdy někdo přeruší kabelové vedení, nebo provede neoprávněný přístup do zařízení. Ochranným kontaktem, tamperem jsou opatřeny veškerá zařízení v PZTS. (Burda, 2017)

Ústředny se dělí čtyř kategorií:

a) smyčkové,

b) sběrnicové s přímou adresací jednotlivých prvků,

c) kombinované,

d) bezdrátové.

Rozdělení se z toho nejobecnějšího hlediska dělí na pevný kabelový poplašný systém a bezdrátový zabezpečovací systém. Bezdrátové systémy jsou v porovnání oproti kabelovým dražší, neboť vyžadují více technologií, častější servisní práce a v průběhu času

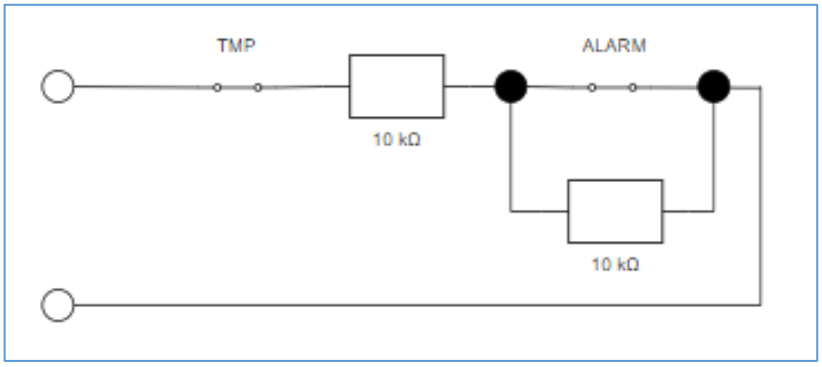
výměnu baterií. Oproti kabelovým systémům mají výhodu např. při instalaci v již postavených domech, kdy není zapotřebí instalace PVC lišt nebo stavební úpravy při instalaci pod omítku. (Maughan, 2016)

2.1.1 Smyčkové

Princip ve smyčkové ústředně spočívá v tom, že každý detektor je do ústředny samostatně připojen pomocí kabelového spojení, tzn. pokud je ústředna vybavena osmi smyčkami, je k ní možno připojit např. osm detektorů. Reálně by šlo na jednu smyčku (svorku) připojit i více detektorů, avšak tyto by následně nešlo rozpoznat. To znamená, pokud se na jednu smyčku připojí dvě čidla, ze dvou místností, tak se následně bude poplach vyhlašovat pro obě místnosti. A to i v případě, že dojde k narušení pouze jednoho čidla. V praxi se tedy počet smyček rovná počtu připojených zařízení. Komunikace v tomto typu ústředen probíhá pouze v jednom směru a sice od detektoru do ústředny, případně od ústředny k aktivnímu prvku. (Burda, 2017)

Funkce a popis je znázorněn na detektoru pohybu. Zařízení, které je do ústředny zapojeno čtyřmi vodiči, kdy dva jsou využity pro kladný a záporný pól napájení a další dva pro komunikaci s ústřednou. V detektoru probíhají tři nejdůležitější stavy, těmi jsou KLID, POPLACH, SABOTÁŽ (přerušení ochranného kontaktu). Aby tento proces mohl probíhat, tak musí být detektor správně zapojen, kdy do jednotlivých obvodů jsou implementovány rezistory (odpory). V praxi se jedná o jednoduché nebo dvojité vyvážení smyčky (obr. č. 2). Detektor má v klidovém stavu sepnuty oba spínače, při přerušení spínače u detekce pohybu dojde rozpojení jednoho z rezistorů a následně ústředna na smyčce změří hodnotu odporu a vyhlásí poplach. V situaci, kdy dojde k přerušení spínače tamperu, zpravidla se jedná o kontakt na krytu detektoru, který se sepne a rozepne při zavření a otevření krytu, je vyslán signál sabotáž. Ústředna na smyčce zaznamená danou hodnotu odporu a dále signalizuje sabotáž, ať už nějakým akustickým prvkem, na klávesnici nebo třeba zasláním SMS na předdefinované telefonní číslo.

Jednou z velkých výhod proudových smyček je kompatibilita detektorů. Zpravidla všechny detektory se zapojují s dvojitým vyvážením a prakticky se jenom mění velikosti odporů instalovaných do čidel dle typu ústředny. Tím pádem je možné použít detektor od jednoho výrobce v ústředně jiného výrobce.

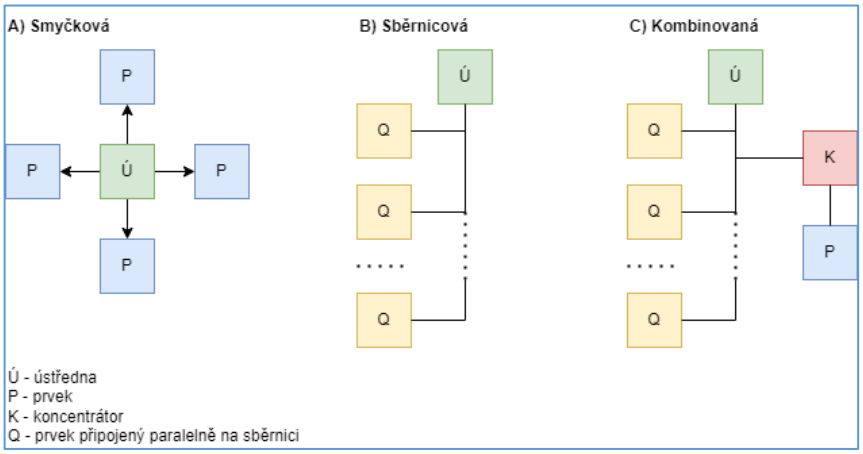


Obrázek 2: dvojitě vyvážená smyčka (vlastní zpracování)

2.1.2 Sběrnicové

Sběrnicové ústředny (obr. č. 3) fungují na principu přímé adresace na sběrnici. To znamená, že všechny koncové prvky jsou připojeny ke sběrnici, typicky datový kabel UPT. Aby systém mohl fungovat, musí mít každé čidlo komunikační modul. Ve většině případů je využito zapojení pomocí čtyř žil kabelu. Stejně jako u smyčkové ústředny jsou dvě žíly využity pro napájení a další dvě žíly slouží jako datová sběrnice. Sběrnice je tedy zapojena do ústředny pomocí dvou kabelů, na obrázku níže označeny jako A a B. Tyto jsou na konci vedení propojeny zakončovacím odporem R. To je z toho důvodu, aby nedocházelo k odrazům signálu a chybám v přenosu dat po sběrnici.

Jednotlivé prvky jsou následně připojeny na sběrnici paralelně. Při narušení ústředna dle adresování vyhodnotí, o jaké čidlo a typ stavu se jedná, a provede konkrétní operaci. (Hladík, 2010)



Obrázek 3: Typy PZTS (Burda, 2017–vlastní zpracování)

Data jsou po sběrnici vysílána v blocích, datových rámcích. Rámec by se dal rozdělit na tři části, ADR, DATA a CRC.

- ADR zastupuje adresu jednotlivých zařízení na sběrnici. Každé zařízení má tedy specifickou identifikační adresu pomocí, které komunikuje s ústřednou.
- DATA zastupují příkazy z ústředny nebo hlášení ze zařízení.
- CRC kontrolní blok v datovém rámci, sloužící ke kontrole přenosu.

Iniciátorem komunikace je v systému vždy ústředna, která vyšle po sběrnici blok dat (datový rámec) adresně směrem k zařízení, kdy se ústředna předmětného elektronického prvku „ptá“ na jeho stav (klid, poplach…). Zařízení opět datovým rámcem „odpoví“ ústředně a odešle stav, ve kterém se aktuálně nachází. (Burda, 2017)

Prakticky to probíhá tak, že ústředna se neustále jednotlivých zařízení dotazuje, v jakém se nachází stavuj, jestli pro *ni nemá něco,* s čím by měla dále pracovat a vyhlásit například poplach.

Nespornou výhodou sběrnicových systémů je redukování počtu a délky tažených kabelů potřebných k zapojení. Další výhodou je, že systém komunikuje se všemi prvky PZTS jedním komunikačním systémem a tím je sběrnice. Jako nevýhodu u sběrnicového systému je nekompatibilnost zařízení, každý výrobce si komunikaci po sběrnici řeší svým způsobem, kdy komunikační moduly v ústředně a jednotlivých prvcích jsou výrobce od výrobce

odlišné. Další nevýhodou je úbytek napětí na sběrnici, toto je způsobeno délkou vedení sběrnice a počtem zapojených zařízení. Problém s úbytkem napětí je řešen tak, že v případě rozsáhlých a vzdálených zapojení jsou do systému zapojeny další zdroje. Následně je část větve sběrnice napájena z hlavního zdroje a další úseky sběrnice jsou poté připojeny na další dodatečné zdroje.

2.1.3 Kombinované

Kombinovaný typ ústředny v oblasti zabezpečovací techniky znamená, jak z názvu vyplývá, že jsou kombinací dvou výše uvedených typů, tedy smyčkové a sběrnicové. Mezi ústřednou a detektory se nachází takzvané koncentrátory nebo linkové moduly. Tyto zařízení se nachází na sběrnici, ta funguje na stejném principu jako u ústředny sběrnicového typu mezi linkou A, B. Koncentrátory jsou následně mezičlánek mezi ústřednou a detektory, jedná se o zařízení, které má svou adresu v rámci sběrnice a dále disponuje daným počtem smyček. Tak jako u smyčkové ústředny se na dané smyčky připojují koncové prvky–detektory. Připojením zařízení na smyčku koncentrátoru získá tento prvek svou adresu, systém zabezpečení je tedy s přímou adresací. (Hladík, 2010)

Kombinovaný typ ústředny je názorně vyobrazen na obrázku č. 3. Z ústředny Ú vede sběrnice, na kterou jsou paralelně připojeny zařízení sběrnicového typu Q, na sběrnici je dále připojen koncentrátor K. Koncový prvek P, například se jedná o detektor, magnetický kontakt apod, je připojen na smyčku koncentrátoru, který v systému slouží jako taková „ústředna“ a vyhodnocuje stavy předmětného detektoru. Následně komunikuje s ústřednou, které zasílá datové rámce obsahující hodnoty–stavy zařízení, které jsou na něj napojeny.

Pro příklad na sběrnici (linku) číslo jedna v ústředně bude připojen koncentrátor, ve kterém bude na smyčce jedna připojen detektor pohybu, pak adresa tohoto čidla bude 1–1–1. Adresace jednotlivých koncových prvků je nezbytná pro jejich určení a naprogramování ústředny. Bez konkrétní, specifické adresy každého prvku v systému by nebylo možné korektně ústřednu naprogramovat a systém, by tak nemohl správně fungovat.

Zabezpečovací systém s kombinovanou ústřednou je velmi výhodný a pohodlný při montáži a samotné instalaci. Je však stěžejní již při návrhu bezpečnostního systému počítat s omezeným počtem smyček na koncentrátorech a také se vzdáleností, kterou je nutno překonat od koncentrátoru ke koncovému prvku. Rovněž je velmi důležité naplánovat vedení sběrnice, neboť požadavek na sběrnici v bezpečnostních systémech je zpravidla, aby byla v přímé topologii sítě. To znamená, aby vedla v linii, nevětvila se.

2.1.4 Bezdrátové

Bezdrátové ústředny jsou z uvedených druhů nejmladším typem ústředen. Tento typ ústředen komunikuje pomocí rádia v pásmu 433 nebo 868 MHz s výkonem pohybujícím se blízko 10 mW. Dosah v prostoru je do 200 metrů v ideálním případě, volné prostranství bez překážek. S využitím v budovách je nutno počítat s úbytkem signálu způsobeným překážkami jako jsou stěny, kovové konstrukce apod. Přenos signálu z čidel do ústředny má zpravidla 8bitů, je kódován a čidla mají 4bitovou adresu. Je snaha čidla navrhnout tak, aby měla v klidovém stavu co nejmenší odběr proudu (do 20 μA), neboť tyto jsou napájeny baterií. Napětí v bateriích je systémem monitorováno a vyhodnocováno, aby v případě nutnosti byl uživatel upozorněn na nutnou výměnu. Upozornění provádí buďto samotné čidlo nebo je signál o nízkém stavu baterie přenesen do ústředny. (Křeček, 2002)

Jako každý systém má i bezdrátová ústředna své výhody a nevýhody. Mezi výhody se jistě nabízí následující:

- nenáročná a rychlá montáž,
- minimální stavební úpravy,
- manipulace a změna lokace jednotlivých prvků,

Mezi nevýhody musíme zařadit:

- častější servisní práce spojené s údržbou baterií,
- vyšší pořizovací náklady jednotlivých modulů,
- omezení vzdálenosti dosahem signálu,
- možnost útoku na PZTS odposlechem nebo rušením radiového signálu.

Radiové ústředny mohou být jednosměrné nebo obousměrné, liší se způsobem komunikace. U jednosměrné komunikace (simplex) se vysílač nachází v čidle a přijímačem disponuje ústředna. V praxi to znamená, že signál je vysílán pouze z čidla do ústředny. Starší systémy tohoto typu nedisponovali žádnou formou kontroly, zda je čidlo v pořádku, jestli nedošlo k sabotáži, poruše atd. Novější systémy již provádí pravidelnou kontrolu prvků vysíláním testovacích telegramů, kdy ověřují přenosovou cestu mezi zařízeními. Systém s obousměrnou komunikací (duplex) je již technicky vyspělejší a každý prvek v systému je již vybaven jak vysílačem, tak přijímačem. Moduly jsou schopny se v dané frekvenci spárovat na volném kanálu a předcházet tak rušení. Duplexní systém je již schopný si ověřit

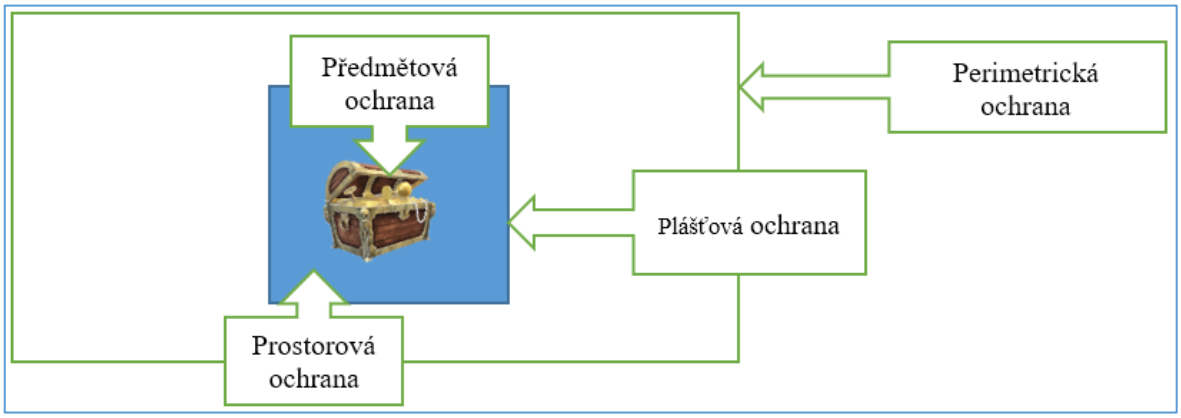
funkčnost připojených zařízení a je schopen lépe vyhodnocovat plané poplachy. Mimo bezdrátová čidla existují ještě další zařízení jako jsou bezdrátové tlačítka, ovládací panely nebo například sirény. (Křeček, 2002)

3 ROZDĚLENÍ PRVKŮ ZABEZPEČOVACÍCH SYSTÉMŮ

Poplachový zabezpečovací a tísňový systém se jako každý jiný sestává z určitých komponent a prvků. Jeden z těchto prvků již práce detailně popsala, ústřednu. Mezi další velmi významné prvky patří detektory.

Pokud je ústředna nazvána jakýmsi „mozkem“ systému, tak v dané terminologii se detektory nejvíce podobají „nervovým zakončením“, neboť právě v těchto zařízeních začíná detekce a je vysílán signál směrem do ústředny. (Maughan, 2016)

Vzhledem k tomu, že se informační technologie a elektronika jako taková neustále vyvíjí a dochází k inovacím a vylepšením, není tomu jinak ani u zabezpečovacích systémů a jejich detektorů. Kvůli rozmanitosti a množství detektorů, je asi nejrozumnější volbou je rozdělit dle způsobu jejich využití. Práce rozděluje jednotlivé prvky dle jednotlivých typů ochrany. V hypotetické situaci, kdy je určen jako předmět zájmu ochrany dokument, který je uložený v trezoru, v zabezpečené místnosti, která se nachází v budově uvnitř areálu ohraničeném plotem, máme všechny typy ochrany. V této situaci je možno využít množství detektorů, které jsou schopny rozpoznat útok pachatele na střežený předmět nebo prostor, a odhalit jej tak ještě předtím, než se k dokumentu vůbec přiblíží.



Obrázek 4: Prostorové rozdělení ochrany (vlastní zpracování)

Na obrázku č. 4 lze vidět dané zóny, které musí útočník překonat, v případě, že je jeho primárním cílem odcizit předmět X (truhla s pokladem). Tento předmět je umístěn v trezoru odkud by musel být pachatelem zcizen, zde je již první (v případě postupu útočníka poslední překážka) možnost zabezpečení předmětu například tíhovým detektorem, z toho vyplývá, že se jedná o **předmětovou ochranu**. Vstup do místnosti s trezorem je opatřen prostorovým detektorem, v tomto případě se jedná o **prostorovou ochranu**. Místnost je samozřejmě situována v budově, do které jsou vstupy jako dveře a okna. Tyto mechanické překážky jsou

opatřeny magnetickými kontakty a otřesovými čidly a je tak tvořena **plášťová ochrana** budovy. A vstup do areálu je tvořen bránou a oplocením, které je střeženo snímačem otřesů, a proto je zde rovněž **perimetrická ochrana**.

Mezi další prvky PZTS, které jsou všeobecně známi a uživatelé je mají neustále na očích jsou ovládací zařízení, jako jsou klávesnice, případně ovládací tlačítka. Samozřejmostí jsou také prvky signalizující poplachové signály z detektorů.

3.1 Plášťová ochrana

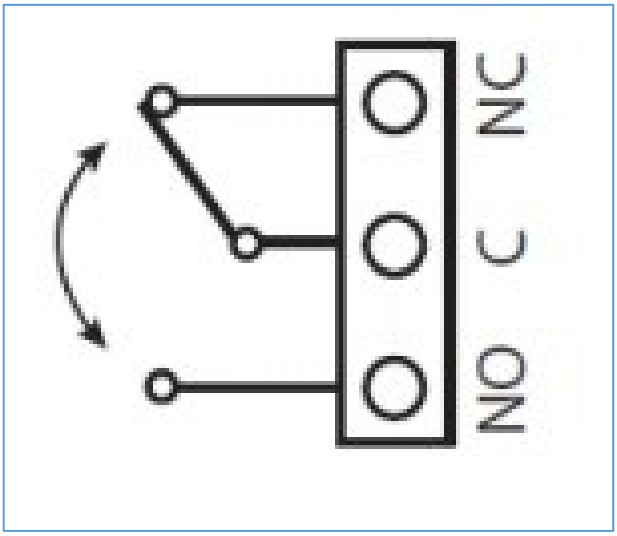
Jak je již uvedené výše jedním z typů ochrany je plášťová ochrana. V tomto případě se jedná zejména o zabezpečení fyzických konstrukcí. Návrh zabezpečení daného objektu spočívá v odhalení slabých míst, které jsou snazší pro vniknutí do objektu nežli například vybourání otvoru ve stěně. Těmito potencionálně slabými (kritickými) místy jsou zpravidla veškeré otvory v plášti budovy. Mezi tyto patří samozřejmě vstupy jako jsou dveře, okna, stropní okna, případně světlíky nebo například ventilační zařízení nebo šachty pro technologie a vzduchotechniku. Aby bylo dosaženo kvalitního zabezpečení objektu, musí splňovat podmínky kompletní plášťové ochrany. Samotná ochrana je koncipována tak, aby byl pachatel detekován při průniku do budovy.

3.1.1 Magnetický kontakt

K základním detektorů využívaných při plášťové ochraně patří magnetické kontakty (dále „MK“). Tento prvek se využívá zejména při zabezpečení mechanicky otevíratelných vstupů jako jsou: dveře, vrata, světlíky, okna. Magnetický kontakt se skládá ze „dvou“ částí, kdy jednu tvoří permanentní magnet a druhou jazýčkový kontakt.

Část s kontaktem je od výrobce zařízení, které je zalisované v plastovém těle kvádrovitého tvaru, zhruba o rozměrech 6 x 1,5 x 1,5 [cm]. Poplachová smyčka v případě MK MAS303 se sestává z dvou nepocínovaných vodičů a je typu NC tzn., že se jedná o smyčku, která je v klidovém režimu spojená s COM kontaktem. Dalším párem vodičů je sabotážní smyčka, která je pocínovaná, ta vyhlašuje sabotáž v případě přerušení vedení těchto vodičů, nebo v situaci, kdy je magnetické pole ovlivněno cizím magnetem. I u smyčky pro sabotáž se jedná o NC kontakt. (MAS 303, 2007)

- COM – kontakt, který se překlápí mezi NC a NO
- NO – kontakt rozpojený v klidovém stavu s kontaktem COM
- NC – kontakt spojený v klidovém stavu s kontaktem COM (Co znamenají zkratky, c2023)



Obrázek 5: Stavy kontaktů (Co znamenají zkratky, c2023)

Magnet se instaluje na pohyblivou část zavíracího mechanismu, tato část je totiž samostatná a není potřeba připojovat vodiči do ústředny nebo koncentrátoru. V ideálním případě se montuje na nemagnetické podklady, aby nedocházelo k rušení magnetického pole. V případě, že není jiná možnost jsou využívány podložky z plastového materiálu. Část prvku s vodiči se připevní na rám okna, zárubeň dveří, tak aby splňovala požadavky dle instalačního manuálu.

Pro příklad u magnetu MAS 303 musí být dodržena mezera mezi magnetem a jazýčkovým kontaktem na nemagnetickém podkladu 3 až 18 mm a na magnetickém 1 až 12 mm, jinak magnetický kontakt nebude pracovat korektně a může docházet k falešným poplachům. (MAS 303, 2007)

Připojení vodičů se provede pomocí dvojitého vyvážení viz. obr. č. 2 na smyčku koncentrátoru nebo ústředny. Výhodou magnetického kontaktu je, že pracuje bez napětí, a proto nepotřebuje přívod napájecích vodičů.

3.1.2 Detektory na ochranu skleněných ploch

Skleněné plochy mají svá specifika a při jejich rozbití vzniká v pevném tělese vlnění. Je více možností, jak takového plochy před případným útokem na tento materiál zabezpečit. Vlnění, které je způsobeno nárazem do skleněné plochy se detekuje čidlem, které se řadí do

kontaktních detektorů. Tyto jsou připevněny přímo na skleněnou plochu. Kontaktní detektor pracuje s piezoelementem naladěným na frekvenci, která vzniká při rozbití skla. Instalace je doporučována 2 až 5 cm od rámu a pro předcházení falešným poplachům se nedoporučuje instalovat na jednoduchá zasklení. (Kupka, 2013)

Mezi dalšími detektory pro ochranu skleněných ploch se vyskytují **aktivní čidla**. Ty v sobě obsahují vysílací a přijímací moduly. Hodnoty klidového stavu skleněné plochy, potažmo elektroniky uvnitř detektoru jsou v něm předem uloženy. Následně pak elektronika uvnitř detektoru vyhodnocuje změny oproti normálu. Nejrozšířenějším typem detektorů v oblasti ochrany skleněných ploch jsou **akustické čidla**. Jak si z názvu každý zvládne odvodit, tak se již nejedná o vyhodnocení vlnění v materiálu, ale o akustický jev. Tříštění skla vyvolává specifický zvuk a s ním spojené akustické vlnění. Uvnitř detektoru je elektronový mikrofon, který je schopen přijímat toto vlnění, které vyhodnocuje a v případě, že se jedná o část spektra typickou pro tříštění skla přejde do poplachového stavu, který odešle do ústředny. (Křeček, 2002)

Moderní detektory tohoto typu jsou schopny detekovat dvě frekvence přicházející s destrukcí skla. Dokážou detekovat nízkou frekvenci vlny nárazu a vysokofrekvenční tříštění skla. Tato vlastnost dokáže eliminovat značnou část falešných poplachů, neboť v případě poplachu musí být detekovány obě frekvence specifické pro rozbití skla. Jako hodně dalších detektorů existují i akustická čidla v bezdrátovém provedení komunikující bezdrátově v protokolu 868 MHz.

3.2 Předmětová ochrana

Předmětovou ochranou se rozumí zabezpečení dotyčných chráněných hodnot, těmi mohou být různé předměty. Typickým příkladem v této kategorii jsou obrazy nebo cennosti. V případě, že dojde k manipulaci s předmětem, detektor svými senzory detekuje pohyb a vyhlásí poplachový stav. Nejrozšířenějším prvkem z kategorie předmětové ochrany je tíhový detektor. Dále se můžeme také setkat s detektorem s akcelometrem, který měří zrychlení potažmo pohyb předmětu. Detektory předmětové ochrany mohou být dle typu předmětu buďto interní, kdy je detektor součástí chráněného předmětu nebo externí, kdy se detektor nachází mimo střežený předmět. V případě externích detektorů je předmět na detektoru položen a působí na něj svou tíhou nebo visí například na háčku. V takových případech se využívá piezoelektrického senzoru, akcelometru nebo tenzometru.

3.2.1 Tíhový detektor s piezoelektrickým senzorem

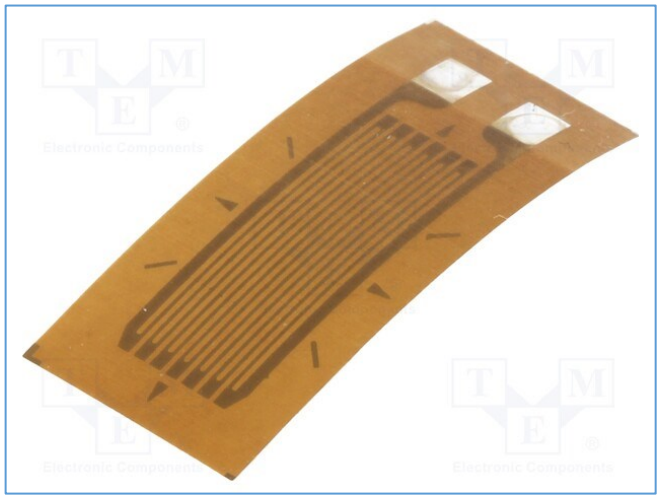
Tento typ tíhového detektoru se používá v závěsových i podložkových detektorech například při střežení uměleckých děl. Předmětný senzor je tvořen zpravidla destičkou, která je vyrobena z piezoelektrického materiálu. Destička je opatřena na protilehlých stranách elektrodami. V případě, že je materiál mezi elektrodami namáhán, stlačován nebo roztahován, tak dochází k deformaci materiálu. Dojde ke zvětšení nebo zmenšení tloušťky materiálu, a tímto se zničí krystalová struktura uvnitř materiálu a dochází k pohybu elektrických nábojů. Posuvy v krystalické struktuře dojde k narušení elektrické neutrality a pod jednou z elektrod se objeví kladný náboj, pod opačnou elektrodou záporný. Takto vznikne tzv. piezoelektrickému jevu. (Burda, 2017)

Při měření napětí multimetrem mezi elektrodami v době stlačení a uvolnění destičky se zobrazí na displeji multimetru několik voltů, napětí však téměř okamžitě po uvolnění zaniká. Po připojení rezistoru na senzor a jeho zatížením například obrazem začne na snímač působit síla F (tíha materiálu). Tím dojde ke vzniku piezoelektrického jevu, kdy v souvislosti s ním vznikne elektrický proud I v podobně proudové špičky, vyrovnají se potenciály a proud zanikne. V tomto okamžiku bude senzor v klidovém režimu, jakmile dojde k naklonění, pozvednutí nebo sejmutí obrazu ze senzoru, vznikne opět proudová špička a detektor vyhodnotí manipulaci s předmětem a vyhlásí poplach. (Burda, 2017)

3.2.2 Podložkový detektor

Využití podložkových detektorů se uplatní například u uměleckých děl jako jsou různé sošky, historické předměty apod. Předmět, který má být zabezpečen se jednoduše položí na podložkový senzor, tento pak měří tíhu, kterou na něj předmět vyvíjí. U tíhových detektorů je rovněž využíváno piezoelektrického jevu nebo tenzometru. Tenzometry měří velikost mechanického napětí na povrchu tělesa. V bezpečnostních systémech se využívá lepících fólií, na kterých je nanesena tenká vrstva vodivých linií viz. obrázek č. 6. Materiál, ze kterého je meandr vyroben má svou danou vodivost ρ, délku L a plochu S. Pro výpočet odporu platí R=p*L/S. Takto vytvořená fólie se lepí na nosník, na kterém je zapotřebí měřit mechanické napětí. Na nosník položíme předmět, čímž dojde k ohnutí nosníku a natažení fólie s vodivými liniemi, změní se tak částečně plocha, průměr a délka. Takto zatížený nosník je v klidovém stavu a má odpor R´.

Jakmile dojde k uvolnění nosníku, nosník se narovná, tenzometr se rovněž vrátí do výchozí polohy a senzor vyhodnotí odpor R, který bude menší než odpor tenzometru v zátěži a dojde k vyhlášení poplachu. (Burda, 2017, Kyncl 2014)



Obrázek 6: Fóliový tenzometr (TENMEX, b. r.)

3.2.3 Akcelerometr

Jedná se o detektory, které jako příčinu pro vznik ohlášení poplachu registrují pohyb. V současné době se jedná o relativně malé zařízení, které je vybaveno akcelometrem. Detektor je napájen baterií, aby nebylo potřeba k němu vést kabelové připojení a komunikuje protokolem o frekvenci 868 MHz. Takto vybavený detektor se připevní na střežený předmět, pokud tedy senzor vyhodnotí pochyb, je také v pohybu objekt zájmu. V situaci, kdy dojde k manipulaci s předmětem, posunutí, naklonění, otřesem apod. akcelometr změří nenulové zrychlení a dojde k vyhlášení poplachu.

3.3 Prostorová ochrana

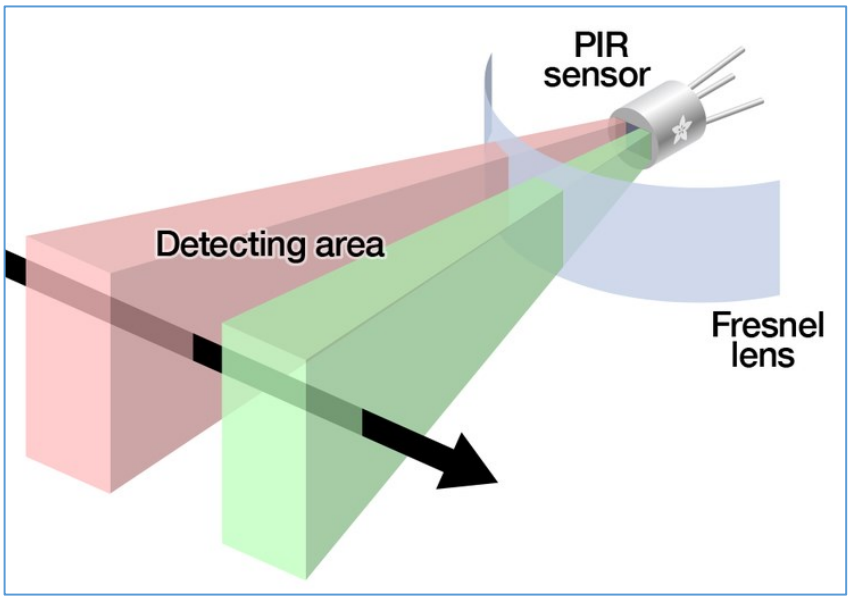
Smyslem a cílem prostorové ochrany je chránit střežený prostor proti neoprávněnému pohybu osob. K tomu se využívají čidla s infračervenými, mikrovlnnými, duálními nebo ultrazvukovými detektory. (Kyndl, 2004)

3.3.1 Pasivní infračervené detektory

V praxi nejvíce využívaným typem čidla je právě čidlo s infračerveným detektorem nesoucí zkratku s anglického „passive infrared“ PIR.

Samotný PIR senzor je dvouslotový, kdy jsou oba vyrobeny ze speciálního materiálu citlivého na infračervené záření. Na diagramu na obrázku č. 7 vidíme, že každý ze senzorů snímá danou oblast. Pokud je senzor v klidovém režimu snímají oba senzory stejné infračervené záření okolí a stěn. V situaci, kdy projde střeženým prostorem člověk a zachytí jej tak jeden ze senzorů vznikne pozitivní diferenciální změna.

Jakmile z oblasti odejde vznikne opět diferenciální změna, ale již záporná. Dané impulzy jsou jev, který PIR čidla detekují a vyvolají poplach. (How PIRs Work, 2014)



Obrázek 7: Diagram PIR senzoru. (How PIRs Work, 2014)

3.3.2 Microwave senzor

Pohybové čidlo s MW (z anglického microwave) senzorem je přesné zařízení schopné rozpoznat polohu pohybujícího se objektu. Detektor využívá elektromagnetického záření a vysílá vlny, které jsou následně detekovány na přijímači. Tyto elektromagnetické vlny a záření se skládají z oscilujících magnetických a elektrických polí. Šíří se velmi velkou rychlostí srovnatelnou s rychlostí světla. Přijímač tohoto zařízení slouží jako analyzátor zpětně se odražených vln. V případě, že se po místnosti objekt pohybuje, tak dochází ke změně frekvence a vlnové délky, přijímač je schopný tuto změnu identifikovat (tzv. dopplerův jev) a vyhodnotí ji jako příčinu pro poplach. MW senzory se dají kalibrovat, aby bylo možné nastavit, jak velké změny v odražených vlnách jsou příčinou pro poplach. Tím se dá redukovat počty falešných poplachů. (How do MW Sensors Work, c2021)

Všechny mikrovlnné senzory pracují v pásmu o frekvenci 0,3 až 40 GHz. Pasivní mikrovlnné senzory mají schopnost detekovat přirozené mikrovlnné záření povrchu. Aktivní

MW čidlo funguje na principu radaru. Je schopno detekovat pohyb i tam kde toho není schopno čidlo PIR, například za výlohou, oknem nebo dveřmi. Moderní pohybové čidla využívají vlastností obou výše zmíněných a vyrábí se takzvaná duální čidla PIR+MW, která jsou vysoce přesné a díky své konstrukci vykazují jen velmi malý počet falešných poplachů.

3.4 Perimetrická ochrana

Pojem perimetrická nebo obvodová ochrana znamená v oblasti bezpečnostních systémů zabezpečení hranice pozemku. Zpravidla se tedy jedná o ohraničení pozemku jako jsou ploty, zdi brány nebo branky, obecně vjezdy. Může se však také jednat o řeku, která sousedí s hranicí pozemku nebo jiné přírodní terénní překážky. Perimetrická ochrana slouží jako první linie pro odrazení pachatele, narušitele. Fyzické překážky jako jsou ploty slouží ke ztížení postupu pachatele a nazývají se jako mechanické zábranné systémy (dále jen „MZS“). Perimetrická ochrana je tedy složena MZS, typicky plotu a detekčních prvků. Mezi elektronické prvky ochrany perimetru se řadí kamerový systém a překážkové detektory. Mezi takové řadíme otřesové senzory, štěrbinové a mikrofonní kabely, tlakové hadice aj. (Kyndl, 2004)

3.5 Ovládací zařízení

Zabezpečovací systém, aby byl uživatelsky přívětiví disponuje ovládacím zařízením. Tento prvek PZTS je velmi důležitý pro uživatele, který je schopen na vyspělejších zařízeních jako jsou **ovládací panely** s displejem, provést mimo ovládaní PZTS také základní diagnostiku. Díky diagnostice je následně uživatel schopen provést opravu nebo ve složitějších případech zavolat servisní firmu. Ovládací panel se stejně jako například koncentrátory připojuje na sběrnici pomocí dvou vodičů A, B a potřebují přívod napájení. Ovládací panely jsou velmi užitečné také pro servisní techniky a mastery systému, kteří mají rozšířené až plné možnosti nastavení. Kdy lze upravovat jednotlivé smyčky, podsystémy, provádět přemostění, úpravu uživatelů atd. Ovládací panely dokáží tak zobrazit celou řadu informací o stavu systému. Slouží ke kontrole a diagnostice. Standartně se využívá pro autorizaci uživatele přístupového kódu (pinu). Panely mohou být modulární a je možno například využít modulu čtecí hlavy. Ta následně může být využita pro načítaní karet sloužících pro autorizaci uživatele.

Mnohem jednodušším zařízením pro ovládání stavu ústředny mohu být klasické **přepínače**, ty je však možné jen přepnout na stav zapnuto nebo vypnuto a nedisponují žádnou další funkcí. Výhodou je, že se dají snadno uschovat a pachatel je tak neuvidí. Lze je tedy využít

při skryté instalaci PZTS. Využití může být například při zabezpečovacím opatření Policie ČR, kdy je monitorován objekt a prioritou je tichý chod PZTS za účelem zadržení osoby pachatele. Dokonalejší verzí obyčejného tlačítka je **bezdrátová klíčenka**. Jedná se o zařízení, které je schopno jednoduchého ovládání systému jako zastřežit, odstřežit, vyhlásit poplach. Existují také klíčenky s programovatelnými tlačítky, těmi lze ovládat pgm výstupy z ústředny.

Samozřejmostí moderní doby je **Sotfware**, ten slouží mj. pro programování ústředny servisním technikem, kde má kontrolu nad celým systémem. Pokud je systém zapojen do sítě je schopen přes vzdálený přístup do konfigurace systému provést úpravy, zobrazit si virtuální i reálnou klávesnici. Pro uživatele existuje nadstavbový software, který má své dané rozhraní, může být webové, ale i aplikační. Zde může uživatel kontrolovat stav systému a rovněž jej ovládat. Má možnost přidávat a editovat uživatele, v některých případech dokonce upravovat podsystémy. V současné době již existují **aplikace** do mobilních telefonů schopné zobrazovat stavy zabezpečovacích systémů, jejich ovládání i omezenou diagnostiku například pomocí **virtuální klávesnice**.

3.6 Signalizační zařízení

Signalizační zařízení mohou sloužit k upozornění uživatele o stavu systému, ale také k vystrašení“ pachatele, jeho následnému zbrklému jednání anebo útěku. Signalizační zařízení může být akustické, kterým je například siréna nebo visuální jako je maják. Existují ve vnitřním i venkovním provedení a mnohdy se jedná o duální provedení, kdy je optické signalizační zařízení realizováno jako součást sirény.

Signalizační zařízení a veškeré jeho součásti musí být umístěny do krytu splňující požadavek na odolnost vůči úderu. Kryt musí být zabezpečen šrouby, případně mechanickým zámkem, který je možné otevřít pouze daným klíčem, nebo specifickým nástrojem. Přívodní kabeláž musí být situována tak, aby ji nebylo možno poškodit bez viditelných stop zničení, poškození nebo vniknutí za účelem vyřazení signalizačního zařízení z provozu. (ČSN EN 50131-4 ED.2, 2019)

4 TECHNICKÉ NÁROKY

Poplachové tísňové a zabezpečovací systémy mají své nároky na funkčnost systému, úplně tím nejzásadnějším je napájení elektrickým proudem, případně akumulátorem, který se však musí neustále monitorovat a provádět servisní výměny. Stejně jako má PZTS své nároky, tak jsou také kladeny nároky na systém. Mezi ně se zařazují například stupně zabezpečení, typ a následný vliv prostředí, komunikace apod.

4.1 Stupně zabezpečení

Pro lepší orientaci ve výstavbě a následujícímu navrhování PZTS jsou stanoveny třídy zabezpečení budov. Dříve byly podle normy CSN EN 50131-1/Z1 stanoveny celkem čtyři stupně zabezpečení: nízké riziko, nízké až střední riziko, střední až vysoké riziko a vysoké riziko.

Od roku 2007, kdy vstoupila v platnost a účinnost norma ČSN P CEN/TS 14383-3 (734400) je definováno celkem pět stupňů zabezpečení, konkrétní rozdělení úrovní je uvedeno níže v tabulce. Stupně zabezpečení jsou členěny z hlediska zabezpečovacích prostředků a dle případné materiální újmy na majetku. (Grémium alarm, 2018)

Tabulka 1: Úroveň rizika a druh zabezpečení. (Grémium alarm, 2018)

Stupeň zabezpečení	Úrovně rizika	Preventivní opatření
1	velmi nízké	Základní mechanické zabezpečení
2	nízké	Zvýšené mechanické zabezpečení
3	střední	Zvýšené mechanické zabezpečení a minimální elektronické zabezpečení
4	vysoké	Rozsáhlé mechanické zabezpečení a střední elektronické zabezpečení
5	velmi vysoké	Rozsáhlé mechanické zabezpečení a vysoké elektronické zabezpečení

4.2 Prostředí

Jedním z dalších důležitých faktorů pro návrh a realizaci zabezpečovacího systému je prostředí, ve kterém bude realizováno. To je velmi důležité z hlediska odolnosti jednotlivých prvků a zařízení, ale také pro správnou funkčnost systému. Také by mohlo dojít ke zničení

prvků i více zařízení působením povětrnostních vlivů na části systému, které nesplňují třídy odolnost např. proti dešti.

Dle normy ČSN EN 50131-1 ed. 2 s účinností od 5/2007 existují celkem čtyři kategorie prostředí viz. tabulka č. 2.

Tabulka 2: Třídy prostředí (ČSN EN 50131-1 ed. 2, 2007)

Třída	Název prostředí	Popis prostředí	Rozsah teplot ve °C
I	Vnitřní	Vytápěná obchodní nebo obytná místa	+5 až +40
II	Vnitřní všeobecné	Přerušovaná vytápěná/nevytápěná místa např. schodiště nebo chodba	-10 až +40
III	Venkovní	Vnější prostředí, komponenty pod střechou	-25 až +50
IV	Venkovní všeobecné	Vnější prostřední, komponenty bez krytí	-25 až +60

4.3 Přenosové cesty

Komunikace mezi zabezpečovacím systémem, respektive ústřednou PZTS a dohledovým a přijímacím centrem Policie České republiky, probíhá výměna informací za využití různých typů přenosových cest. Dle typu ústředny a dalších komponent může komunikace probíhat v režimu simplex nebo duplex. Každý typ přenosové cesty má své výhody, nevýhody, náročnost na instalaci a spolehlivost. Dle specifikace a požadavků na objekt se mohou lišit nároky. V případě DPPC u PČR je například požadavek a podmínka mít dvě přenosové cesty, jednu hlavní a záložní pro případ výpadku. Dojde-li pak k výpadku jedné z přenosových cest, komunikace nadále probíhá po záložní trase. Toto je velmi výhodné například v místech, kde je horší nebo kolísavý signál. Mezi aktuálně nejvyužívanější přenosové cesty se řadí přenos po radiové síti, síti mobilních operátorů, ethernetu případně intranetu, a tedy vnitřní podnikové síti jako například resortní datová síť ministerstva vnitra „HERMES“. Dříve, ale ještě i v dnešní době se využívá komunikace po pevné telefonní síti.

Komunikace v **radiové síti** se může řadit mezi jednu z nejspolehlivějších přenosových cest. Avšak pro správný a bezproblémový chod musí být vybudována radiová síť s celoplošným pokrytím v dané oblasti. K tomu slouží tzv. retranslátory (opakovače), to jsou aktivní síťové prvky, které jsou schopny přijmout zašuměný signál a poté ho vyslat dál zesílený a opravený.

Retranslátory se zbudovávají zpravidla na vysílačích na vyvýšených místech zejména na vrcholcích v terénu. Aby byla komunikace možná musí být ústředna vybavena radiovým modulem.

V rámci **ethernetové** (internetové) sítě, které je rovněž velmi často využíváno, z důvodu dostupnosti téměř ve všech domácnostech a institucích, je zapotřebí aby ústředna disponovala IP modulem, ten slouží právě pro přenos informací po internetové/intranetové síti. Pro komunikaci se využívá TCP/IP protokolu a je nutnost přidělení IP adresy, masky podsítě a výchozí brány pro dané zařízení správcem předmětné sítě.

Obdobná situace nastává v případě využití komunikace přes internetové připojení prostřednictvím mobilního operátora tzv. GSM (Global systém mobile). Ústředny tohoto typu musí být vybaveny GSM modulem, do kterého se zavede SIM karta, která zprostředkovává komunikaci. Velkou výhodou tohoto typu přenosové cesty je, že není nutnost vybudování rozsáhlé sítě jako například u radiového přenosu. Sítě mobilních operátorů dosahují téměř celoplošného pokrytí ČR, a tak lze teoreticky využít kdekoliv, samozřejmě se najdou místa se špatným signálem, kde je potřeba využít jinou přenosovou cestu nebo zřídit vysilač pro mobilní síť.

5 SHRNUTÍ TEORETICKÉ ČÁSTI

Teoretická část práce je věnována přiblížení se oblasti poplachovým a tísňovým systémům, kdy je zejména zaměřena na oblast právního ukotvení. Zde se jedná zvláště o právní normy vydané Úřadem pro normalizaci. Normy jsou v ČR doporučující, mnohdy však navazují na zákony ČR. Mezi nejzásadnější normy řešící problematiku PZTS patří ČSN EN 50131 a její části, kterých má 13. V dalších kapitolách práce byly definovány základní pojmy týkající se poplachových zabezpečovacích a tísňových systémů, jejich architektura a rozdělení jednotlivých prvků. Zde bylo provedeno rozdělení ústředen a jednotlivé typy popsány, z čehož vyplynulo, že nejpraktičtější ústřednou, je ústředna kombinovaná využívající výhody ostatních typů. Práce dále pojednává o možných způsobech zabezpečení dle typu požadované ochrany, ke které se váže správný výběr detektoru. Základním prvkem prostorové ochrany je čidlo PIR, ideálně v duálním provedení například s MW senzorem. Díky teoretické části tak jsou známy potřebné vlastnosti a parametry jednotlivých prvků, které budou využity v analýze a návrhu zebezpečovacího systému objektu v praktické části bakalářské práce.

II. PRAKTICKÁ ČÁST

6 POPIS OBJEKTU

Objekt, který byl pro potřeby práce vybrán je reálným v rámci Policie České republiky, avšak jeho název ani lokalizace nebude uvedena z bezpečnostních důvodů. Samotné místo zvoleného objektu je ze stejných důvodů upraveno, byly změněny názvy ulic a sousedících staveb, tak aby nebylo možno objekt lokalizovat. Areál, v němž předmětná budova sídlí je rovněž upraven, a stejně tomu je i u půdorysu objektu. Pro danou problematiku je však stěžejní členitost objektu, místností kanceláří a jejich využití.

6.1 Dispozice objektu

Předmětný objekt je situován v cípu křižovatky. Hranice areálu tedy tvoří, ze dvou stran silnice a ze severní strany se nachází sportovní hala, která lemuje celou severní stranu. Samotný areál je tvořen budovou ve tvaru písmene „L“. Prostor doplňující areál do obdélníku je tvořen parkovištěm, kde je výjezd/vjezd z jižní strany. Vjezdová brána je vnořena do 3 m vysokého zděného oplocení. Jedná se o zděnou dvou podlažní budovu, bez suterénu. Budova má šíři obvodových (venkovních) stěn 45 cm, nosné vnitřní stěny mají tloušťku 30 cm, příčky jsou zděné o tloušťce 15 cm. Okna jsou plastová s dvojsklem. Výška stropu v místnostech je 300 cm. Podlahy v budově jsou tvořeny z různých materiálů, dlažba, parkety nebo linoleum. Dveře v místnostech jsou zpravidla ze dřeva (výjimka zbrojní sklad apod.) a zavěšeny na kovových zárubních. Budova má sedlovou plechovou střechu, ve které se nenachází průlez z půdních prostor. Místnost pro technologie se nachází v 1. NP v rohu objektu.

Z hlediska stavební dispozice objektu se posuzuje: konstrukce objektu, lokalita, prostředí, stavební otvory, režim provozu, stávající zabezpečení. (Kyncl, 2014)

6.2 Mapový podklad

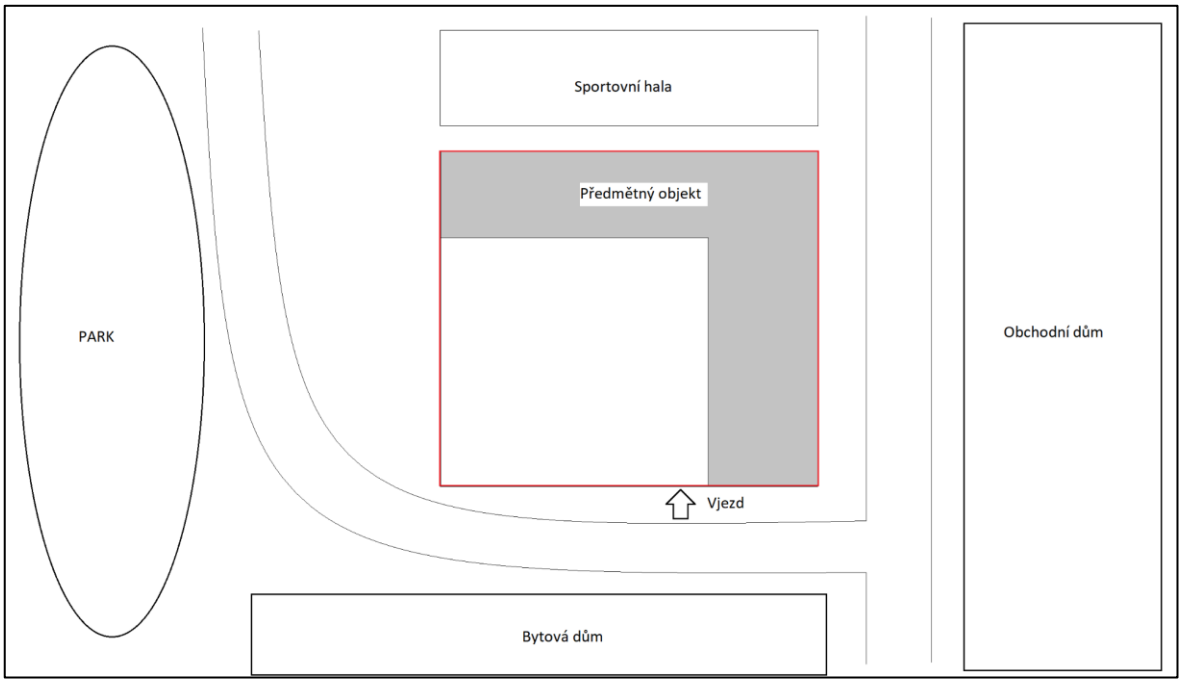
Objekt Policie ČR (dále jen „PČR“) sousedí s následujícími objekty, situační plán znázorněn na obrázku č. 8.

I. **Sever** – přes průchod (chodník) mezi budovami s objektem PČR sousedí po celé šíři severní strany sportovní hala.

II. **Jih** – přes ulici se nachází bytové domy, jedná se řadovou zástavbu se čtyřmi vchody do budovy.

III. **Východ** – na této straně je volnější prostor, kde se přes ulici nachází volně přístupný park s dětským hřištěm a odpočinkovou zónou.

IV. **Západ** – přes ulici se zde nachází velký obchodní komplex s obchody nabízejícími nejrůznější zboží.



Obrázek č. 8: Situační plánek (vlastní zpracování)

Na obrázku výše je červenou barvou vyznačen předmětný areál s objektem PČR. Bílá plocha uvnitř areálu slouží jako parkoviště pro služební vozidla a menší dopravní prostředky, jako jízdní kola, motorky, elektro koloběžky a další. Vjezd je situován, jak je znázorněno z jižní strany, kdy se jedná o výsuvnou bránu. Další odstavné plochy, zejména pro zaměstnance a návštěvy se nachází na západní straně areálu. Ulice na východní straně je rušnější a je zde hustší provoz, zejména kvůli obchodnímu domu. Druhá ulice vedoucí podél západní a jižní strany je poměrně klidná. Budova se nachází v relativně klidné oblasti, kde nedochází k rušení veřejného pořádku, avšak v obchodním domě se často řeší kapesní a drobné krádeže.

7 ANALÝZA OBJEKTU

Analyzovaný objekt PČR, je současně využíván jen z části, kdy je obsazeno jen asi 30% kapacity budovy. Do budoucnosti se v rámci restrukturalizace počítá s plným využitím budovy a naplnění kapacit místností, tak aby došlo ke zlepšení chodu a optimalizace pracovních procesů v rámci působnosti PČR.

Stávající poplachový zabezpečovací a tísňový systém, který je v budově využíván je jen částečný, lokální. Objekt tedy není řádně zabezpečený, ale pod ochranu jsou vzata pouze některá pracoviště. Ústředna NX8 (obrázek č. 9), která je v objektu nainstalována je již starší a pro rozšíření o další zařízení a prvky nevhodná. Vzhledem k tomu, že kapacita kanceláří není plně využívána jsou zabezpečeny pouze některé z nich. Ve 2.NP je pro zabezpečení místnosti využito přenosového zařízení FA101, které slouží zároveň jako objektové zařízení (ústředna). Dochází tak k navyšování počtu ústředen, místností s technologiemi a tříštění zabezpečení na více systémů. Konkrétní zařízení a prvky jsou popsány v dalších kapitolách týkajících se jednotlivých typů ochranu.

Obrázek 9: Ústředna NX8 (vlastní, 2023)

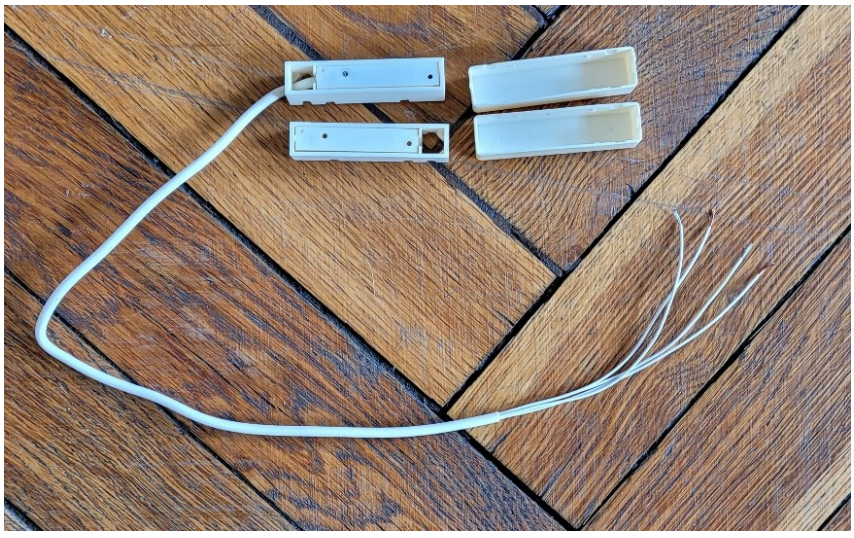
Na obrázku č. 9 se v plechové skříni nachází ústředna NX8. Jako většina ústředen se skládá z několika komponent, v levé části se nachází ústředna a vpravo nahoře zdroj napájení, pod kterým je prostor pro akumulátor.

7.1 Perimetrická

Objekt se nachází na veřejném prostranství, kdy je vnější oblast budovy tvořena pochozími plochami a vozovkou. Není tak možno z více jak 50 % zabezpečit oblast tak, aby byl případný útočník detekován ještě předtím, než dosáhne plášťové ochrany. Tuto službu by do jisté míry mohl zajišťovat kamerový systém, nicméně v aktuální podobě zabezpečení není vybudován. Na protější straně areálu, v místě parkoviště, slouží jako perimetrická ochrana zděný tři metry vysoký plot s mechanickou vjezdovou bránou.

7.2 Plášťová

Plášť budovy je tvořen obvodovými stěnami, přičemž dvě z nich jsou kryty dispozicemi areálu, kdy se nacházejí za jeho zdmi. Severní a východní hranice budovy je tak volně přístupná, stejně tak část jižní a západní strany. Ze všech strany se na budově nacházejí okna, nejsou opatřeny žádnou mechanickou zábranou jako mříže apod. Do samotné budovy je možno vstoupit 2 vchody. Jeden ze vstupů je situován z ulice na jižní straně vedle vjezdu, kde se nachází recepce. Druhý vchod, který slouží pouze pro zaměstnance, se nachází uvnitř areálu. V rámci PZTS jsou zabezpečeny oba vchody do budovy magnetickým kontaktem MAS 203.



Obrázek 10: Magnetický kontakt MAS 203 (vlastní, 2023)

Na obrázku č. 10 je zadokumentován magnetický kontakt MAS 203. Na levé straně se nachází dva „domečky“ pro MK a magnet, vpravo jsou dva kusy krytek.

7.3 Prostorová

Prostorová ochrana je v objektu částečně zbudována formou elektronického zabezpečení. V 1. NP jsou zabezpečeny prostory recepce, zbrojního skladu a okolních kanceláří. Ve 2. NP je zabezpečen sklad techniků a archiv. Prostory jsou zabezpečeny starším typem PIR detektoru (obrázek č. 11). Prostorovými čidly jsou zabezpečeny celkem čtyři místnosti a zbrojní sklad, což je pro zabezpečení budovy naprosto nedostatečné.

Obrázek 11: PIR detektor (vlastní, 2023)

Jako ovládací zařízení k systému slouží klávesnice NX–124a (obrázek č. 12). jedná se o standartní klávesnice bez displeje s led signalizací stavů ústředny. Veškeré zařízení je připojeno do ústředny NX8, která je umístěna v technologické místnosti. Pro přenos dat na DPPC slouží přenosové zařízení FA101T, které zprostředkovává komunikaci s ústřednou a přenos.

Systém byl instalován asi před 20 lety, v současné době je již zastaralý a nevyhovující dnešním standardům a potřebám, zejména v rámci očekávaného rozšíření využitelnosti budovy.

Obrázek 12: Klávesnice NX–124a (vlastní)

7.4 Předmětová

Předmětová ochrana v objektu je využita v souvislosti se zbrojních skladem. Jedná se o zděnou místnost, vchod do místnosti je opatřen jedněmi mřížovými a druhými oplechovanými dveřmi, každé zvlášť uzamykatelné. V samotné místnost se nenachází žádný další otvor. Vnitřní dveře jsou opatřeny magnetickým kontaktem a vnitřní prostory jsou chráněny PIR detektorem. Zbraně se ukládají do kovové trezorové skříně.

7.5 Režim

V současné době je objekt, jak již bylo výše uvedeno využíván pouze z části. Není zde stálá služba, je zde recepce s recepčním s klasickou pracovní dobou PO-PÁ do 15:30 hod. Část objektu využívá dálniční oddělení, které má sice 24hodinovou pracovní dobu, ale v případě výjezdů a hlídkování je oddělení uzavřeno a zabezpečeno. Za objekt nese odpovědnost vedoucí směny v daný den, který má mj. za úkoly kontrolovat areál, vjezd do areálu a vydávat zbraně oproti podpisu v knize zbraní uložené v místnosti pro dozorčí. V místnosti je rovněž umístěna ústředna a přenosové zařízení PZTS.

Naplněním kapacity objektu a rozšíření o oddělení cizinecké policie bude zavedena dozorčí služba s nepřetržitou pracovní dobou. Recepce bude zrušena a bude zde vytvořena místnost pro dozorčí službu s veškerým potřebným vybavením. Technologie PZTS již nebude v místnosti pro dozorčí, ale v technologické místnosti.

7.6 SWOT Analýza

Tento typ analýzy je nejvíce využíván pro zhodnocení vnitřních a vnějších faktorů ovlivňujících úspěch organizace. SWOT analýza je velmi univerzální metodou, jednou z nejpoužívanějších technik vůbec a lze ji aplikovat téměř na jakýkoliv řešený problém. Z toho důvodu byla zvolena i ke zhodnocení stavu zabezpečení na předmětném objektu. Název techniky SWOT je akronym z počátečních písmen faktorů ovlivňujících výsledek analýzy.

- **Strengths** – silné stránky podniku,
- **Weaknesses –** slabé stránky podniku,
- **Opportunities –** příležitosti, možnost zlepšení,
- **Threats –** hrozby, odkud hrozí riziko a je nutno si zde dávat pozor.

V rámci práce byla využita SWOT analýza pro zhodnocení bezpečnostního stavu budovy, níže jsou uvedeny faktory a vyhodnocení metody.

Silné stránky

Objekt Policie ČR sám o sobě už je jakýmsi ochranným prvkem, kdy jeho napadení případného útočníka odradí. Stavebně dobrá plášťová ochrana, více jak polovina je tvořena samotnou budovou o šíři obvodových stěn 45 cm. Zbylá část, kdy se jedná o perimetr je oplocena 3 m vysokým zděným plotem. Částečně vybudovaný zabezpečovací systém, napojený na DPPC. Malý počet možností pro vniknutí do budovy, bez podsklepení.

Slabé stránky

Pachatel může vniknout do budovy nezabezpečenými okny, následně má relativně snadný pohyb po chodbách, kde není žádné zabezpečení a po místnostech bez detektorů pohybu. Absence venkovního elektronického zabezpečení a osvětlení parkoviště. Časové úseky, kdy se v budově nikdo nenachází, zejména v nočních hodinách, kdy jsou policisté na hlídkové službě nebo řeší protiprávní incidenty.

Příležitosti

Zpracování návrhu a následná realizace PZTS. Instalace kamerového systému, zejména v zájmu perimetrické ochrany. Reorganizace výkonu služby a zavedení nepřetržité kontroly budovy dozorčí službou. Využití moderních technologií pro kontrolu vstupu.

Hrozby

Budova se nachází v blízkosti obchodního centra. Přístupu na hranici pozemku (plášti budovy) není možno, kromě přístupu přes parkoviště, nijak zabránit, protože se jedná o veřejné prostranství. Mezi vnější hrozby musíme zařadit přírodní vlivy a technické závady, které mohou být příčinnou např. vzniku požáru.

7.6.1 SWOT matice

Tabulka 3: SWOT matice (vlastní zpracování)

Silné stránky	Slabé stránky
➢ Objekt PČR ➢ Malý počet míst vniknutí (okna) ➢ Částečný PZTS ➢ Mechanicky odolná plášťová ochrana (budova, plot)	➢ Lehce přístupná okna v 1. NP ➢ Žádné venkovní elektronické zabezpečení ➢ Venkovní osvětlení ➢ Časové úseky bez dozorčí služby nebo vrátného
Příležitosti	**Hrozby**
➢ Návrh a realizace PZTS ➢ Instalace kamerového systému ➢ Zřízení dozorčí služby ➢ Využití moderních technologií	➢ V blízkosti obchodní centrum (krádeže, poškození) ➢ Snadný přístup k budově ➢ Přírodní vlivy (vichřice, povodeň) ➢ Technické závady (požár)

7.6.2 Vyhodnocení analýzy

Pro správné vyhodnocení SWOT analýzy je zapotřebí přiřadit jednotlivým faktorům bodové ohodnocení. Silné stránky a příležitosti jsou ohodnoceny na stupnici od 1 do 5, přičemž hodnota 1 je nejnižší a 5 nejvyšší. U slabých stránek a hrozeb je hodnocení v záporných číslech, kdy -1 je nejmenší hrozbou (slabou stránkou) a hodnota -5 nejvyšší.

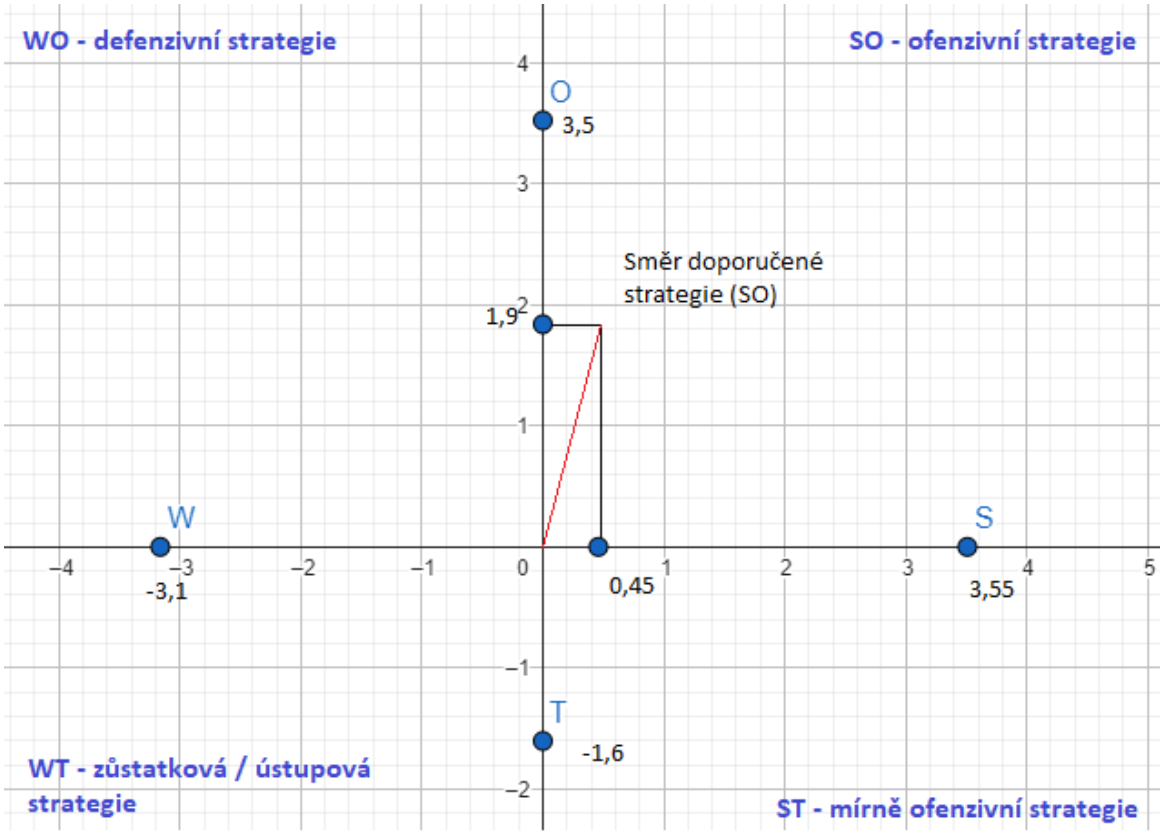
V tabulce č. 4 byly faktorům přiřazeny hodnoty a každému z nich byla dána váha jakou daný faktor ovlivňují. Součet vah v dané kategorii musí být vždy roven 1.

Tabulka 4: Vyhodnocení SWOT analýzy (vlastní zpracování)

Faktory	**Hodnocení**	**Váha**	**Celkcem**
Silná stránka			
Objekt PČR	4	0,4	1,60
Možnosti vniknutí	3	0,15	0,45
Částečný PZTS	2	0,15	0,30
Mechanická odolnost	4	0,3	1,20
		Celkový součet	**3,55**
Slabá stránka			
Snadný přístup k oknům	-2	0,2	-0,4
Absence venkovního osvětlení	-4	0,3	-1,2
Absence venkovního el. Zabezpečení	-3	0,25	-0,75
Časové úseky bez personálu	-3	0,25	-0,75
		Celkový součet	**-3,1**
Příležitosti			
Vybudování PZTS	4	0,4	1,6
Instalace kamerového systému	3	0,3	0,9
Zřízení dozorčí služby	4	0,2	0,8
Využití moderních technologií	2	0,1	0,2
		Celkový součet	**3,5**
Hrozby			
v místě se nachází obchodní komplex	-2	0,3	-0,6
Snadný přístup k budově	-1	0,2	-0,2
Přírodní vlivy	-1	0,2	-0,2
Technické závady	-2	0,3	-0,6
		Celkový součet	**-1,6**

Přiřazením hodnot a vah jednotlivým faktorům bylo získáno jejich matematické vyjádření. Pro lepší přehlednost a představu jsou hodnoty zpracovány do grafického vyjádření. V grafu jsou zaneseny všechny získané hodnoty a dále se na osách nachází body, po odečtení protilehlých faktorů. Spojnice mezi 0 a průsečíkem těchto bodů nám udává doporučený trend pro zlepšení bezpečnosti budovy.

Dle doporučeného směru strategie, prostor pro zlepšení je zejména v oblasti příležitostí, kdy velká hodnota a váha je přiřazena vybudování zabezpečovacího systému. Hned v dalším pořadí, je z analýzy patrné, že bezpečnost značně ovlivní zřízení stálé dozorčí služby a instalace kamerového systému.



Obrázek 13: Grafické vyjádření zjištěných hodnot analýzou (vlastní pracování)

Jak z tabulky č. 4, tak z obrázku č. 13 je patrné, že objekt má již v současné podobě své silné stránky, což nám dokazuje hodnota 3,55. Na druhou stranu hodnota slabých stránek dosahuje téměř na hodnotu silných stránek a je zde tedy prostor pro zlepšení. Z grafu na obrázku č. 13 vyplývá doporučený směr strategie SO–ofenzivní strategie. Díky převažujícím silným stránkám je reálně možné zlepšit bezpečnost objektu využitím nabízených příležitostí. Vzhledem k vysoké hodnotě příležitostí, které místy korespondují se slabými stránkami, dojde jejich využitím ke snížení hodnoty slabých stránek, což následně bude mít za následek zlepšení celkového stavu zabezpečení objektu.

8 NÁVRH ZABEZPEČNÍ OBJEKTU

V následující kapitole bude proveden návrh bezpečnostního řešení budovy. Prvotním cílem je zabezpečit objekt komplexním zařízením, ve kterém budou integrovány všechny potřebné zabezpečovací systémy. Proto bude zvolen typ ústředny, která disponuje technickými možnostmi řešení pro elektronické zabezpečení poplachovým systémem a systémem EKV.

8.1 Trade FIDES

Pro zabezpečení objektu je v návrhu zvolen systém s ústřednou ASSET. Jedná se o zabezpečovací zařízení vyráběné a dále vyvíjené firmou Trade FIDES, a. s.

Tento podnik patří k jednomu z největších dodavatelů komplexních integrovaných bezpečnostních systémů v ČR. Na trhu působí již 25 let a mezi její zákazníky patří např. Policie a Armáda ČR, ČEZ, banky a další. Firma Trade Fides nabízí hardwarové komponenty a softwarové aplikace, které nabízí komplexní řešení bezpečnostních systémů. V návrhu zabezpečení bude využito systému ASSET, jedná se o systém poplachového a zabezpečovacího systému s možností implementace systému EKV a dohledového video systému. Veškeré informace získané systémem budou přenášeny na DPPC Krajského ředitelství Policie ČR. Zde je zabezpečen nepřetržitý dohled nad DPPC integrovaným operačním střediskem. Pro dohledové centra je firmou dodáván systém DPPC LATIS, který je grafickou nadstavbou a splňuje požadavky dle normy ČSN EN 50518. (FIDES, b. r.)

8.2 Komponenty a prvky zabezpečovacího systému

Ústředna ASSET 804 Z spolu s přenosovým zařízením PZR-1 bude umístěna v technologické místnost v rohu budovy. V technologické místnosti budou dále umístěny linkové moduly pro nejbližší detektory. Návrh zabezpečení počítá s kompletní plášťovou ochranou prvního patra (přízemí). V každé z místností, kde se nachází skleněná výplň se bude nacházet detektor tříštění skla GLASSTEK 456 od firmy PARADOX. V případě, že je skleněná výplň (okno) otevíratelná bude opatřena magnetickým kontaktem MAS 303. Ve všech místnostech a na chodbách v prvním nadzemním podlaží budou nainstalovány detektory pohybu PARADOX DG65+. Vstupní dveře do budovy budou opatřeny magnetickým kontaktem, elektrickým zámkem a dvojící čteček Asset 602, které pro svou činnosti vyžadují univerzální modul Asset 6.20. Ten musí být nainstalován v blízkosti předmětných dveří. Linkové moduly LML-8 budou z části umístěné v technologické místnosti a dále pro pohodlnější instalaci dle rozmístění detektorů. Vzhledem k tomu, že se

jedná o již vystavěnou budovu není možné kabeláž klást pod omítku, a proto povede v PVC kabelových lištách. Objekt bude rozdělen na více podsystémů, které bude nutno v průběhu služby ovládat, a proto budou dle potřeby instalovány klávesnice KMU4N, ty zároveň slouží jako akustická výstraha v případě poplachu nebo poruchy na zařízení. V místnosti dozorčí služby bude nainstalováno tísňové tlačítko, jednoduché zařízení, které při stisku vyvolá poplach.

V dalších odstavcích jsou uvedeny jednotlivé komponenty navrhovaného zabezpečovacího systému. V kapitole 8.4 je graficky znázorněn plán objektu s rozmístěním jednotlivých prvků ochrany. Detektory jsou instalovány dle technických parametrů, v předepsané výšce, tak aby byly schopné řádně plnit svou funkci.

Ústředna ASSET 804Z

Ústředna pro použití v členitých a rozsáhlých objektech. V kovové skříni je kromě ústředny integrovaný zdroj PWR 4A (obrázku č.14 v dolní části). Do skříně lze umístit akumulátor do velikosti 40Ah. Skříň, průmyslové pc, připojené linkové moduly, klávesnice a další přípojné zařízení jsou určeny pro prostředí třídy II dle normy ČSN EN 50131-1 ed. 2 pro teplotní rozsah -10 °C až +40°C. Stupeň krytí je IP 30. Na obrázku č. 14 můžeme vidět v horní části Expandér v3, který slouží k rozšíření ústředny o další tři sběrnice. Napájecí zdroj 5 V slouží jako měnič napětí z 12 V na 5 V. Průmyslový PC je uprostřed v levé části, k němuž je zprava připojen koncentrátor (linkový modul) LML-8. Ústředna díky expandéru v3 disponuje 4 sběrnicemi RS485, kdy na každou z nich je možné připojit až 30 linkových modulů. Linkový modul disponuje 8 dvojitě vyváženými vstupy. Celkem je tedy možno na jednu sběrnici připojit až 240 vstupních smyček (čidel). (Rámcová dohoda, 2019)

Ústředna je nejdůležitějším zařízením celého systému, a proto musí být chráněna proti neoprávněnému přístupu cizích osob.

Obrázek 14: Asset 804Z (Rámcová dohoda, 2019)

Zařízení bude umístěno v technologické místnosti, která bude mimo dobu servisních a jiných prací vždy zastřežena. Pro technologickou místnost bude vytvořen samostatný podsystém. Ústředna splňuje certifikaci NBÚ, tato je uvedena níže v tabulce č. 5.

Tabulka 5: Ústředna ASSET 804Z certifikace NBÚ (NBÚ, 2023)

Identifikační číslo TP	**Název výrobku**	**Výrobce a držitel jméno**	**Držitel adresa**	**Držitel město**	**Kategorie použití**	**Počet bodů dle BS**
T1018/2022	Ústředna PZTS a EKV	Trade FIDES, a.s.	Dornych 57	617 00 Brno	3	SS91=3

Platnost certifikace NBÚ platí do 16. 12. 2024

Klávesnice KMU4N

Jedná se o ovládací panel k systému ASSET. Umožňuje přihlášení uživatele pomocí hesla, karty nebo jejich kombinací pro zvýšení zabezpečení. Po přihlášení technika pomocí technického hesla lze provést diagnostika systému. Displej je dvouřadý o délce až 20 znaků.

Pod displejem se nachází skupina 6 LED, které signalizují stavy ústředny. Při poplachu nebo poruše vydává rovněž akustický signál. (FIDES, 2022)

Obrázek 15: Klávesnice (FIDES, 2022)

Klávesnice jakožto hlavní ovládací prvek budou nainstalovány u vstupních dveřích do objektu. Dále u dveří zbrojního skladu a u schodiště ve druhém podlaží. Další klávesnice budou rovněž nainstalovány před vstupem do jednotlivých oddělení v rámci objektu. Rozložení ovládacích prvků je znázorněno v plánech objektu v kapitole 8.4. Na obrázku č. 16 jsou uvedeny úplné technické parametry ke KMU4N.

Klávesnice KMU4N je systémová a připojuje se na sběrnici RS-485, druhou možností je připojení přes rozhraní TTL.

Napájecí napětí	+10 V DC až +14,5 V DC						
	Čtecí hlava	**Jas displeje**	**Podsvícení tlačítek**	**Klidový stav[1] [mA]**		**Max. signalizace[2] [mA]**	
				+10 V DC	**+14,5 V DC**	**+10 V DC**	**+14,5 V DC**
Odběr proudu	**Nepřipojena**	**Standardní**	**Úsporné**	64	54	82	65
			Plné	82	71	105	85
		Zvýšený	**Úsporné**	87	69	113	77
			Plné	108	87	134	102
	Připojena	**Standardní**	**Úsporné**	116	91	134	98
			Plné	134	109	155	123
		Zvýšený	**Úsporné**	147	126	163	114
			Plné	156	108	181	139
Rozměr krytu (š x v x h)	165 x 143 x 24 mm						
Rozměry displeje (š x v)	123 x 23 mm						
Hmotnost	445 g						
Barevné provedení krytu[4]	Bílá, černá, stříbrná						
Materiál krytu	**Čelo** Sklo						
	Tělo Plast						
	Záda Plast						
Pracovní teplota	-10 °C až +40 °C						
Třída prostředí	II (Vnitřní všeobecné)						
Stupeň zabezpečení	4						
Akustická signalizace	Polyfonní bzučák						
Vizuální signalizace	6x LED						
Displej	2 x 20 znaků, Jednobarevný						
Rozhraní	1x RS-485 (systémová), 1x TTL						
Počet a typ smyček[3]	1x bezpotenciálová smyčka určená pro technologii dveří, 1x bezpotenciálová smyčka určená pro tísňové tlačítko						
Počet a typ výstupů	**Počet**	**Typ**	**Popis**				
	2x	OC GND	+75 V DC / 1,5 A, 2 W				

Obrázek 16: KMU4N technické parametry (FIDES, 2022)

Detektor pohybu DG65+

Na zabezpečení prostorové ochrany vnitřních prostor objektu budou použity PIR detektory pohybu Paradox DG65+. Jedná se o infrapasivní detektor firmy Paradox se čtyřnásobným prvkem. Jedná se o pohybový detektor s klasickým 4 vodičovým zapojením pro rozeznání poplachu a tamperu (sabotáže). Na vhodných a nezbytných místech bude k čidlu využito příslušenství a sice univerzálního držáku SB469 Universal Swivel Mount B. (Eurosat, b. r.)

Detektor DG65+ je umístěn v plastovém krytu, který je možno připevnit do univerzálního držáku. To je výhodné zejména v případech, kdy je třeba čidlo přesně nasměrovat.

Obrázek 17: Pohybový detektor a univerzální držák (Eurosat, b. r.)

Technické parametry:

Typ senzoru	Čtyřnásobný infračervený element
Geometrie senzoru	ISG (Interlock)
Pokrytí: 110 °	12 x 12 m
Montážní výška	2,1 m do 2,7 m
Provozní teplota	0 °C do + 50 °C
Napájení	11 až 16 VDC
Proudová spotřeba	15 mA max.
EMI / RFI odolnost	10 V /m od 10 MHz do 1 GHz
Čočka	Druhá generace Fresnelových čoček, LODIFF
Rychlost detekce	0,2 m do 3,5 m / sek.
Poplachový výstup	Tvar A relé 10mA/28VDC, N.C.
Ochranný kontakt	N.C., 150mA/28VDC

Obrázek 18: Technické parametry DG65+ (Eurosat, b. r.)

Detektor tříštění skla GLASSTREK 456

V prvním nadzemím podlaží (přízemí) v místnostech se skleněná plochou budou nainstalovány detektory tříštění sklad od výrobce Paradox GLASSTREK 456.

Jedná se o akustický detektor se senzory detekující nízké i vysoké frekvence vzniklé při nárazu i porušení skla. Mezi hlavní vlastnosti patří: Analýza slyšitelného pásma a infrazvuku, Imunita proti VF rušení, nastavitelná citlivost na vzdálenost 4,5 až 9 metrů.

Samozřejmostí je možnost využití testovacího zařízení pro správnou instalaci a kontrolu funkčnosti detektoru. Takovým zařízením je např. TestTrek 459 od firmy PARADOX. (Eurosat, b. r.)

Technické parametry:

Napájení	9 -16 Vdc
Odběr	25 mA
Rozměry	9 cm x 6,6 cm x 2,5 cm
Váha	100 g
Výstupní relé	150 mA, 28 Vdc
Tamper	150 mA, 28 Vdc
Operační teplota	- 20°C do + 50°C
Typ mikroprocesoru	12 / 8- bitový

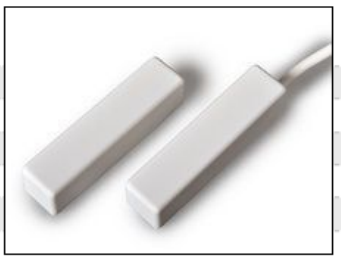
Obrázek 19: Detektor tříštění skla GLASSTREK 456 s parametry (Eurosat, b. r.)

Magnetický kontakt MAS303

Vhledem k tomu, že se nejedná o novostavbu a v budově se již nachází plastová okna, budou pro jejich ochranu použity magnetické kontakty pro povrchovou montáž. V případě novostaveb nebo u výměny oken je vhodné využít situace a navrhnout magnetické kontakty zapuštěné přímo do oken a rámů. U kontaktů pro povrchovou montáž je více možností upevnění. To se provádí například nalepením lepidlem, oboustrannou páskou, ale z praxe je známo, že lepené magnety časem odpadnou a je potřeba servisních prací. Ideální volbou pro montáž je tedy připevnění šrouby, vruty z neferomagnetického materiálu. Při montáži je velmi důležité postupovat dle manuálu a je nezbytné přesné umístění magnetického kontaktu a magnetu, neboť pracovní vzdálenost je 2 až 22 mm. (Eurosat, b. r.)

Magnetický kontakt se skládá z více částí, pro montáž jsou vyrobeny plastové „domečky“. Ty se připevní na místo detekce a následně se dovnitř vloží magnetický kontakt a magnet.

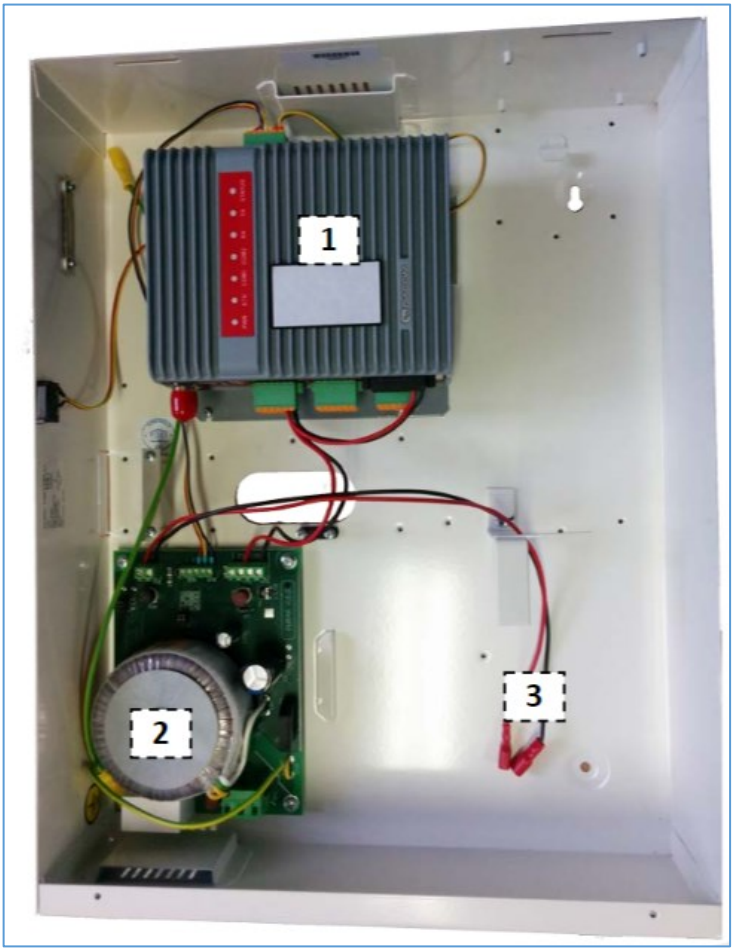
Technické parametry



Rozsah pracovních teplot	-40 až +70°C
Relativní vlhkost	max95% při 40°C
Atmosférický tlak	66 - 106 kPa
Krytí	IP65
Rozměry (vnější)	54 x 13 x 13mm
Hmotnost	68g vč. kabelu 3m
Spínané napětí/proud/výkon	max.50V/max.250mA/max.3W
Počet sepnutí (12V, 20mA)	2.10^9
Odpor stav sepnuto/rozepnuto	max.2Ω /min.10^9Ω
Délka přívodu	3m
Izolační odpor mezi smyčkami	min 10^9Ω

Obrázek 20: Magnetický kontakt MAS 303 (Eurosat, b. r.)

Přenosové zařízení PZR-1



Obrázek 21: Objektové zařízení PZR-1 (Exner, 2015)

Zařízení zvolené pro obousměrný přenos komunikace mezi ústřednou a DPPC PČR je stejně jako ústředna od firmy Trade FIDES a. s. Toto zařízení se skládá z několika komponent

umístěných v plechové skříni, kde se nachází zdroj PWR 4A a místo pro akumulátor o velikosti až 18 Ah. Zařízení PZR-1 je určeno dle normy ČSN EN 50131-1 ED.2 pro vnitřní prostředí a splňuje stupeň krytí IP 30. **RipEX F** je hlavním komponentem přenosového zařízení. Jedná se o objektové zařízení, které má technické parametry a řešení umožňující zabezpečení menších objektů. Spojení se systémem LATIS SQL probíhá standartně po rádiovém nebo LAN rozhraní. Lze jej ovšem připojit i pomocí telefonní linky. Splňuje krytí IP 40. Pro připojení detektorů lze využít 8 dvojitě vyvážených vstupů. S ústřednou PZTS se propojuje pomocí sériového portu RS232. Na obrázku č. 21 jsou komponenty rozmístěny následovně 1 – RipEX F, 2 – zdroj PWR 4A, 3 – místo pro akumulátor. (Exner, 2015)

Zařízení bude v rámci realizace PZTS umístěno v technologické místnosti spolu s ústřednou. Na obrázku č. 22 jsou uvedeny technické parametry zařízení RipEX F.

Obchodní označení	RipEX F
Typ	RipEX-400
Výrobní kód	RipEX-400F
Napájení	11-15V=
Spotřeba	max. 41,4W
Komunikace s PCO	LATIS SQL3
Komunikační kanály - LAN - telefonní linka	- rádiový modem
Vstupy	- 4 nevyvážené vstupy (I1-I4) - 8 dvojitě vyvážených vstupů (10 kΩ klid, 20 kΩ poplach) - telefonní komunikátor: CID, 4+2 - RS232 (spel, spel2, ASSET,…)
Podsystémy	- 4
Výstupy	- LAN, - 2 ks relé - Tranzistorový výstup (otevřený kolektor) -
Konfigurační software	FDC (Fides Device Configurator)
Rozměry	50mm x 150mm x 118mm
Hmotnost	1,1 kg

Obrázek 22: Technické parametry RipEX F (Exner, 2015)

Linkový modul LML-8

Koncentrátor neboli linkový modul LML-8 slouží k připojení různých typů detektorů do systému ASSET. Modul je připojen na sběrnici RS 485 a vyžaduje napájení 12 V DC.

Linkový modul disponuje celkem 8 vstupy pro připojení detektorů. Na desce linkového module se nachází DIP přepínač (modrá barva), kterým se určuje adresa na sběrnici. Adresa musí být pro každý modul univerzální, nesmí se shodovat s jiným modulem, jinak dojde ke kolizi a následné ztrátě komunikace. (Trade FIDES, 2014)

Linkový modul (expander) má celkem pět svorek pro napětí +/-, sběrnice je označená písmeny a, b.

Obrázek 23: Linkový modul LML-8 (Trade FIDES, 2014)

Zdroj PWR 4A

Pro napájení zařízení a dobíjení baterie je PZR-1 vybaveno zdrojem PWR 4A. (Exner, 2015)

Obrázek 24: Napájecí zdroj (Exner, 2015)

Jedná se o relativně malé zařízení, které je však doplněno o akumulátor až do velikosti 55 Ah, který má hmotnost cca 18 kg.

Napájecí zdroj je vybaven výstupy na svorkách S, B, Z, které pro připojení vyhodnocují stavy sítě, baterie, zdroje napájení.

Napájecí zdroj (PS)	…	typ A
Stupeň zabezpečení	…	3
Třída prostředí	…	II (vnitřní všeobecné)
Napájení	…	230V~ 50Hz
Příkon	…	max. 80W, 100VA
Odběr proudu	…	max. 430mA
Účiník	…	0,8
Krytí	…	IP 00
Pracovní teplota	…	-10°C až 40°C

Výstup DC:
Jmenovitý výkon … 58W
Výstup SV6 … dobíjení baterie nastavitelné 13,2 až 14,1V/ nastavení dobíjecího proudu propojkami J1 a J2: 0,75-1,1-1,5-1,85A
Akumulátor olověný (SD): 12V, vhodná kapacita 42Ah pro dru-hý a 55Ah pro třetí stupeň zabezpečení
ochrana proti hlubokému vybití akumulátoru 10,5V
Výstup SV4: výstupy typu OC, sepnuto = OK, rozpojeno = závada
- S … indikace výpadku sítě se zpožděním 50s (pozn.:<160V~), zpoždění hlášení lze zkrátit na cca 2s osazením propojky J3
- B … indikace poruchy baterie se zpožděním 8s
… indikace nízkého napětí baterie (<11,8V) se zpožděním 4min
- Z … indikace poruchy napájecí jednotky (PU) se zpožděním 8s
… indikace nízkého napětí napájecího výstupu se zpožděním 8s

Výstup SV5: výstupy /S a Tamper pro zařízení NCL
Výstup SV2,3 … napájecí výstup, maximální napětí podle nastavení dobíjení baterie, minimální napětí 11V, jmenovitý proud do 3,5A podle nastavení proudu dobíjení, maximální proud 4A krátkodobě, zvlnění max. 0,6V, ochrana proti přepětí ~17V,

Účinnost	…	68% při poloviční zátěži
Provozní teplota	…	-10 až 40°C … prostředí vnitřní všeobecné
Provozní vlhkost	…	max. 85% … prostředí vnitřní všeobecné
Rozměry	…	max. 146 x 106 x 51 mm
Montáž	…	rozteč 135 x 95 mm, sloupky M4 x 10 mm
Hmotnost	…	cca 1015g

Obrázek 25: Technické parametry zdroj (Exner, 2015)

8.3 Komponenty pro systém elektronické kontroly vstupu

V rámci obměny starého zabezpečovacího systému proběhne i vybudování systému EKV. S tím se počítalo již při návrhu a výběru typu ústředny. Zvolený Asset 804 Z má hardwarové a technické možnosti pro implementování systému EKV. Instalace EKV probíhá připojením univerzálního modulu Asset 6.20 na sběrnici, ke kterému se připojí dvojice čteček Asset 602. Tyto lze připojit pomocí rozhraní RS232, RS422 nebo Wiegand. Čtečky umožňují čtení bezkontaktních RFID karet a čipů.

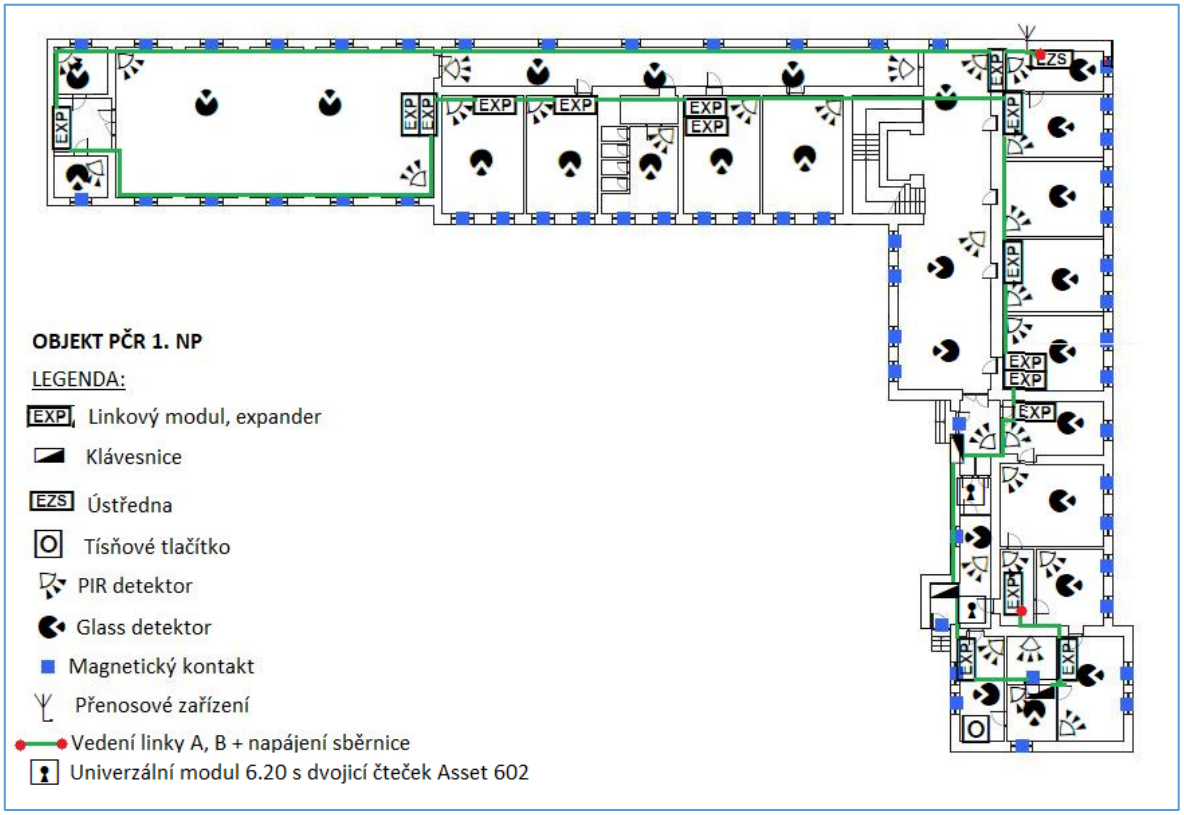
Univerzální modul Asset 6.20 disponuje šestí výstupy pro připojení detektorů a lze jej využít například pro připojení čidel nebo magnetických kontaktů.

čtečka Asset 602

univerzální modul Asset 6.20

Obrázek 26: modul a čtečka EKV (FIDES, b. r.)

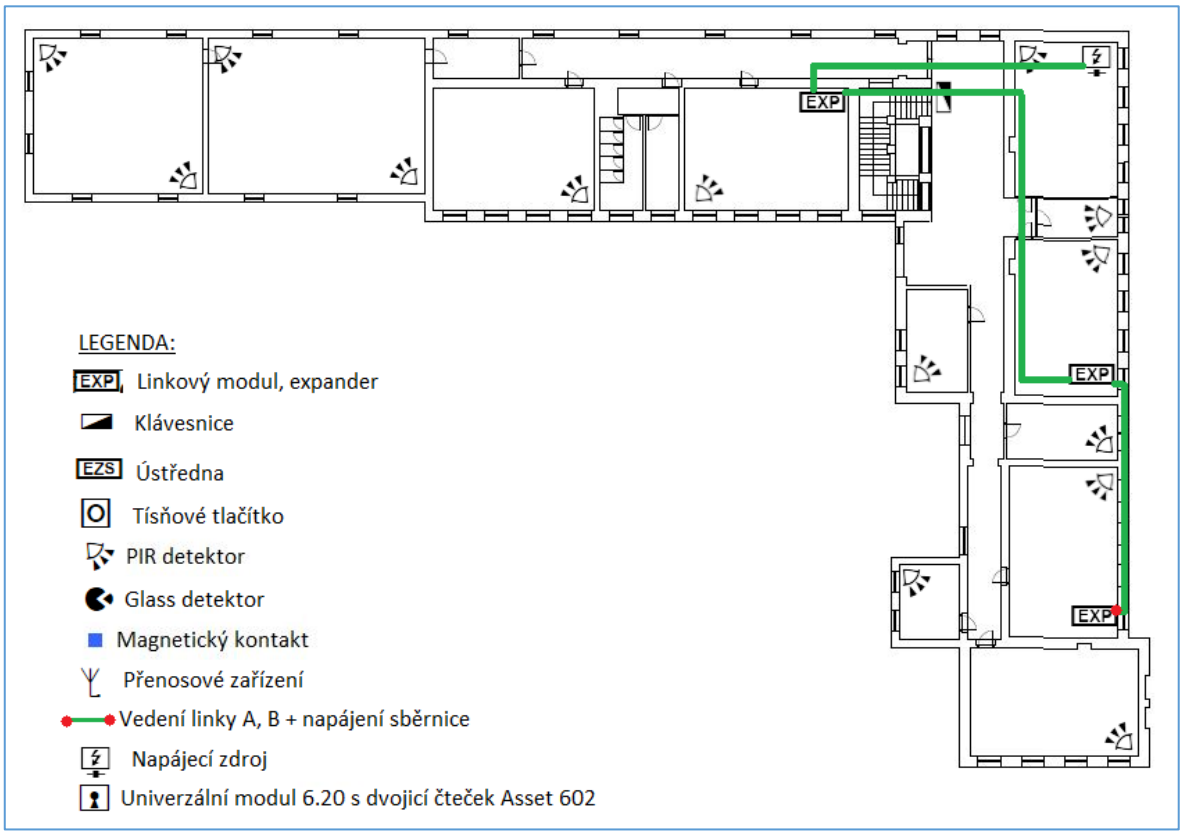
8.4 Grafické rozložení komponent a jednotlivých prvků



Obrázek 27: Plán objektu 1. NP (vlastní zpracování)

Na obrázku č. 27 a 28 lze vidět rozvržení prvků PZTS. Jednotlivé prvky jsou popsány v přiložené legendě. Sběrnice vyznačená zelenou linkou je tažena bez přerušení a větvení, jedná se o sběrnicovou topologii.

Pro každé patro byla vyčleněna jedna linka, zbylé dvě linky zůstaly neobsazeny, ty lze využít při budoucích úpravách a rozšíření systému.



Obrázek 28: Plán objektu 2. NP (vlastní zpracování)

8.5 Kompletace zabezpečovacího systému

Zabezpečovací a tísňový systém pro objekt Policie ČR je navrhnut a zpracován v plánech na obrázcích č. 27 a 28. Zejména v prvním podlaží se nachází velké množství detektorů. Z důvodu kompletní ochrany pláště přízemí a velkému počtu okenních ploch, bylo v návrhu použito mnoho magnetických kontaktů. Naopak ve druhém patře vzhledem k tomu, že objekt není přístupný z okolních budov nejsou magnetické kontakty navrhnuty. V 1. NP se téměř ve všech prostorách (místnosti, chodby) nachází PIR a GLASS detektory. Velkému počtu těchto prvků odpovídá také vcelku vysoký počet linkových modulů. Mezi další zařízení s nutností nastavení své jedinečné adresy patří klávesnice a univerzální modul pro vstupy do budovy. Celkovým počtem adresných zařízení došlo téměř k zaplnění kapacity jedné sběrnice (linky).

Již zde je vidět, že byla dobře zvolena ústředna s celkovým počtem 4 sběrnic (linek), které mohou být využity pro případné rozšíření o další zařízení. V návrhu zabezpečení byly využity linky 2, pro každé patro byla využita jedna.

Tabulka 6: Cenová kalkulace návrhu PZTS (vlastní zpracování)

Název zařízení	Počet kusů 1. NP	Počet kusů 2. NP	Celkový počet (ks)	Cena za kus v Kč	Cena celkem Kč
Ústředna ASSET 804 Z	1	0	1	22650	22650
Přenos. z. PZR-1	1	0	1	46246,20	46246,20
Linkový modul	16	3	19	2516,80	47819,2
Klávesnice KMU4N	3	1	4	8409,50	33638
PIR DG65+	27	14	41	958	39278
Glasstrek 456	27	0	27	885,72	23914,44
MAS 303	56	0	56	509	28504
Tíseň tlač.	1	0	1	966	966
Univer. modul. 6.20	2	0	2	5172,75	10345,50
Čtečka 602	4	0	0	5626,50	22506
Napájecí zdroj PWR533	0	1	0	14338,50	14338,5
Celková cena					**290 205,84**

Výše zpracovaná tabulka počítá s dostupnými cenami v obchodě Eurosat, dále pak s rámcovou smlouvu policejního prezidia z roku 2019 a veřejně dostupných smluv z portálu smlouvy.gov.cz. Ceny jsou uvedeny v korunách českých, a to včetně DPH. V cenové kalkulaci není zahrnut spotřební materiál jako vruty, hmoždinky, PVC lišty, kabeláž a opotřebení nářadí. Rovněž zde není úhrada za práci. V případě objednávky se tedy musí počítat s vyšší cenou.

8.5.1 Podsystémy

Objekt PČR má svá specifika, a proto je nutné jej rozdělit do více podsystémů (zón), nestačí mít celou budovu jen ve stavu pod ochranou nebo vyjmutou z ochrany. Předmětná budova má specifické místnosti, konkrétně se jedná o zbrojní sklad a místnost s technologiemi, kde

je umístěna ústředna PZTS. Každá z těchto místností bude míst svůj vlastní podsystém, rozložení můžeme vidět v příloze P I, kde zbrojní sklad (C) je vyobrazen žlutou barvou a technologická místnost (D) červenou. Zbylá část přízemí je dalším podsystémem (A), v příloze označeno modrou barvou. Veškeré detektory ve druhém nadzemní podlaží jsou posledním čtvrtým podsystém (D). Na podsystém A je navázaná technologická místnost, aby v případě zastřežení došlo i k zastřežení podsystému D a byla tak splněna plášťová ochrana. Uživatelé mají své přidělené kódy, policisté služební průkazy a zaměstnanci průkaz zaměstnance, ty zároveň slouží jako čipové karty. Pomocí čipové karty a hesla se na klávesnici provede dvoufázové ověření, tím dojde k autorizaci uživatele. Po přihlášení může uživatel následně ovládat podsystémy, které mu přidělil MASTER systému. Uživatel má svá oprávnění, které určuje MASTER, jedná se o funkce jako změna svého hesla nebo rušení poplachů. Naopak MASTER uživatel může na klávesnici provádět přemostění detektorů (systém bude daný detektor ignorovat), diagnostiku, změnu hesel uživatelů apod.

8.5.2 Software

Asset config

Pro programování ústředen ASSET firma Trade FIDES vyvinula a stále aktualizuje program Asset config. V tomto programu se nastavují veškeré detektory, linkové moduly, klávesnice a přiřazují se jim adresy, dle nastavených přepínačů. Vytváří se zde podsystémy, jejich provázání, zpožděné smyčky apod. Přes Asset config se také provádí upgrade firmware jednotlivých zařízení. Běžný uživatel do tohoto programu nemá přístup, nastavení provádí servisní technik, v rámci policie technik z Odboru technické ochrany PČR.

Fides device configurator

Další z programů potřebných ke zprovoznění systému PZTS. V tomto programu se zejména nastavují spojení ethernet, GSM, radiové nebo telefonní. Přes FDC se programuje například zařízení PZR-1.

LATIS client

Latis client je aplikace sloužící pro dohled nad objekty. Tuto aplikaci má na svém počítači obsluha DPPC. Má zde seřazené veškeré přidělené objekty, které monitoruje a v případě poplachu nebo poruchy provádí úkony dle instrukcí. Přes LATIS client je možnost provádět na dálku operace jako zastřežení, odstření, restart zařízení, vyčítání stavu podsystémů, sledování signálu apod.

9 SHRNUTÍ PRAKTICKÉ ČÁSTI

Praktická část práce byla rozdělena do tří kapitol. První kapitola byla věnována přiblížení objektu z hlediska zasazení budovy v městské zástavbě. Situačnímu rozložení areálu a zhodnocení stavebního řešení objektu. V druhé kapitole byla provedena analýza současného stavu zabezpečení budovy, včetně popisu a uvedení jednotlivých prvků zabezpečení. Pro vyhodnocení současného stavu bezpečnosti budovy byla vybrána SWOT analýza, kterou bylo zjištěno, že současný stav z komplexního hlediska není úplně nejhorší, ale je zde prostor pro zlepšení. Vybudování PZTS vyšla jako nejlepší příležitost pro vylepšení současného stavu bezpečnosti objektu. V poslední kapitole věnované návrhu PZTS, bylo navrženo vybudovat systém na ústředně ASSET 804 Z s radiovým přenosem (PZR-1) a záložní trasou přes ethernet. Dále byla vyčíslena orientační cena zařízení a komponent, která bez práce a spotřebního materiálu dosáhla hodnoty 290.206, - Kč s DPH. V závěru poslední kapitoly bylo uvedeno softwarové vybavení pro systém ASSET.

ZÁVĚR

Cílem bakalářské práce byl návrh nového zabezpečení budovy Policie České republiky v souladu se stanovenými požadavky. První část bakalářské práce tvoří část teoretická, která je rozdělena do čtyř kapitol. Zde bylo zakomponováno vše podstatné, aby čtenář získal základní přehled o řešené problematice v oblasti zabezpečovacích a tísňových systémů. Stěžejním výstupem druhé části bakalářské práce, praktické, je analýza a návrh bezpečnostního systému pro předmětný objekt.

V první kapitole teoretické části je problematika uvedena do kontextu v rámci právního ukotvení, kde je stěžejní technická norma ČSN EN 50131 a její části 1 až 13. Je zde vysvětlen pojem PZTS jako takový, jeho účel a význam. V další části teorie se práce věnuje principům fungování zabezpečovacích systémů jejich úskalím a omezením. Kapitola dále rozděluje jednotlivé typy ústředen a vysvětluje jejich výhody a nevýhody při instalaci a následném provozu systému. Vzhledem k tomu, že práce se zabývá poměrně širokým a technicky náročným tématem, byla myšlenka, v teoretické části, přiblížit jednotlivé prvky PZTS, tak aby byly obsaženy ty, které se využijí v praktické části při řešení daného problému. Cílem tedy nebylo čtenáři představit veškeré komponenty, detektory a jiné prvky ochrany. Jednotlivým zařízením je věnována celá třetí kapitola této bakalářské práce. V poslední části teorie jsou uvedeny jednotlivé stupně zabezpečení, třídy prostředí a typy přenosových cest pro komunikaci ústředny s dohledovým poplachovým a přijímacím centrem.

Hned v prvním oddíle praktické práce je uvedeno účelové využití řešeného objektu, který je následně podroben analýze aktuálního stavu zabezpečení a stavebně technického řešení budovy a okolního prostředí. Byl proveden rozbor současného zabezpečovacího systému a jeho komponent. Z hlediska bezpečnosti byl řešený objekt podroben SWOT analýze, ze které vyplynulo, že objekt má své silné stránky převyšující slabé stránky, nicméně existují příležitosti, které mohou bezpečnost objektu výrazně vylepšit. Mezi těmito příležitostmi vyšla nejhodnotněji výstavba nového PZTS. Kapitola osmá je věnována samotnému návrhu zabezpečovacího sytému, požadavkům na systém a návrhu jednotlivých komponent. Jako hlavní prvek systému byla zvolena ústředna ASSET 804Z od firmy Trade FIDES, a. s., která disponuje technickými možnostmi pro integraci všech navržených systémů PZTS a EKV. Celý systém je navržen tak, aby jednotlivé komponenty byly připojeny na sběrnici, přes kterou probíhá veškeré zasílání dat od linkových modulů s připojenými detektory a modulů EKV. Při návrhu PZTS bylo počítáno se zavedením nepřetržitého směnného provozu

a zřízení stále služby, z těchto důvodů nebyla do návrhu zahrnuta perimetrická ochrana, neboť je zde velké riziko planých poplachů spojených s nesprávnou manipulací s PZTS.

Přínos práce lze vidět zejména ve zhodnocení a vyřešení zabezpečovacího systému objektu. Současný stav elektronického zabezpečení je zastaralý s malým počtem detekčních prvků a bez systému kontroly vstupu. V případě, že by opravdu došlo k reorganizaci výkonu služby a navýšení využitelnosti budovy, mohl by návrh zabezpečení posloužit jako jeden z možných způsobů řešení.

SEZNAM POUŽITÉ LITERATURY

BURDA, Karel, 2017. Základy elektronických zabezpečovacích systémů. Brno: Akademické nakladatelství CERM. ISBN 978-80-7204-967-7.

Co znamenají zkratky, c2023. I4wifi [online]. Praha: 100MEGA Distribution [cit. 2023-03-29]. Dostupné z: https://www.i4wifi.cz/cs/faq/351-co-znamenaji-zkratky-na-rele-no-nc-com

ČESKO, 2005. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: Sbírka zákonů České republiky. ročník 2005, číslo 412. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-412

ČSN EN 50131-1 ed. 2, 2007. Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky: Výstražná zařízení. Praha – Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 334591.

ČSN EN 50131-4 ED.2, 2019. Poplachové zabezpečovací a tísňové systémy: Výstražná zařízení. Praha – Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 334591.

EUROSAT: Detektory, kontakty [online], b. r.. Eurosat CS [cit. 2023-04-13]. Dostupné z: https://1url.cz/Vr6C8

EXNER, Robert, 2015. Přenosové zařízení PZR -1. Brno. Dostupné také z: https://adoc.pub/penosove-zaizeni-pzr-1.html

FIDES [online], b. r. Brno: Trade FIDES [cit. 2023-04-12]. Dostupné z: https://www.fides.cz/

FIDES: Asset 602 [online], b. r. Brno: Trade FIDES [cit. 2023-04-12]. Dostupné z: https://www.fides.cz/asset-602

FIDES: KMU4N Ovládací panel [online], 2022. Brno: Trade FIDES [cit. 2023-04-12]. Dostupné z: https://www.fides.cz/files/kmu4nw-datasheet.pdf

Grémium Alarm: Příručka zabezpečení objektu, 2018. In: Mvcr.cz [online]. Praha: Agentura ČAS [cit. 2023-04-01]. Dostupné z: https://www.mvcr.cz/soubor/prirucka-zabezpeceni-objektu.aspx

HLADÍK, Drahoslav, 2010. Elektronické zabezpečovací systémy a elektronická požární signalizace. SOUE Plzeň. Dostupné také z: https://www.souepl.cz/wp-content/ucitele/hladik/opvk2009/Ukazka-skripta/Skripta_ukazka.pdf

How do MW Sensors Work, c2021. Raypcb [online]. Shenzhen: Shenzhen World Exhibition & Convention Center [cit. 2023-03-30]. Dostupné z: https://www.raypcb.com/microwave-motion-sensors/

How PIRs Work, 2014. Adafruit [online]. New York: https://www.adafruit.com/ [cit. 2023-03-30]. Dostupné z: https://learn.adafruit.com/pir-passive-infrared-proximity-motion-sensor/how-pirs-work

KŘEČEK, Stanislav, 2002. Příručka zabezpečovací techniky. Blatná: Blatenská tiskárna. ISBN 80-902938-2-4.

KUPKA, Andreas, 2013. Installationsanleitung: FU7300 [online]. [cit. 2023-03-29]. Dostupné z: https://1url.cz/NrYQr

KYNCL, Jaromír, 2014. Bezpečnost objektu ve světle moderních technologií. Praha: Komora podniků komerční bezpečnosti České republiky. ISBN 978-80-260-7115-0.

KYNDL, Jiří, 2004. Projektování bezpečnostních systémů. I. díl. Zlín: Univerzita Tomáše Bati. ISBN ISBN 8073181657.

ManagementMania: SWOT analýza, c2011-2016. Https://managementmania.com/cs [online]. Praha: Educius [cit. 2023-04-12]. Dostupné z: https://managementmania.com/cs/swot-analyza

MAS 303: Instalační manuál, 2007. TZK s.r.o. [online]. Honeywell spol. s r.o. [cit. 2023-03-29]. Dostupné z: https://1url.cz/xrYQu

MAUGHAN, Joel, 2016. Home Security Systems: Home Security Tips Revealed [online]. Lulu Press [cit. 2022-11-15]. ISBN 9781329981973. Dostupné z: https://play.google.com/books/reader?id=rUPVCwAAQBAJ&pg=GBS.PT4&hl=en_US

Nároní bezpečnostní úřad [online], 2023. Praha: NBÚ [cit. 2023-04-12]. Dostupné z: https://1url.cz/4r8rl

RÁMCOVÁ DOHODA: Integrované bezpečnostní systémy, 2019. Policejní prezidium. Praha. Dostupné také z: https://1url.cz/gr6at

Technické normy, c1998-2023. *VARNET s. r. o.* [online]. Praha: VARNET [cit. 2023-02-13]. Dostupné z: https://www.varnet.cz/dokumenty/podpora/technicke-normy/

TENMEX: Fóliový tenzometr TFS10/120-PTENMEX, b. r. In: TME: Electronic components [online]. [cit. 2023-03-30]. Dostupné z: https://1url.cz/zrYBk

TRADE FIDES, 2014. Linkový modul LML-8. Brno. Dostupné také z: https://adoc.pub/2014-popis-vyrobku-pro-system-asset-manual-technika-systemu.html

Závaznost norem, c2020. Česká komora AIT [online]. Praha: ČKAIT [cit. 2023-04-01]. Dostupné z: https://www.ckait.cz/zavaznost-norem

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

DPPC Dohledové přijímací a poplachové centrum

EKV Elektronická kontrola vstupu

FDC Fides device configurator

GSM Global System for Mobile communication (globální systém pro mobilní komunikaci)

IOS Integrované operační středisko

MK Magnetický kontakt

MW Mircrowave (mikrovlnný)

MZS Mechanické zábranné systémy

NBÚ Národní bezpečnostní úřad

PČR Policie České republiky

PIR Passive infrared (pasivní infračervený)

PVC Polyvinylchlorid (jeden z nejpoužívanějších plastů)

PZTS Poplachový zabezpečovací a tísňový systém

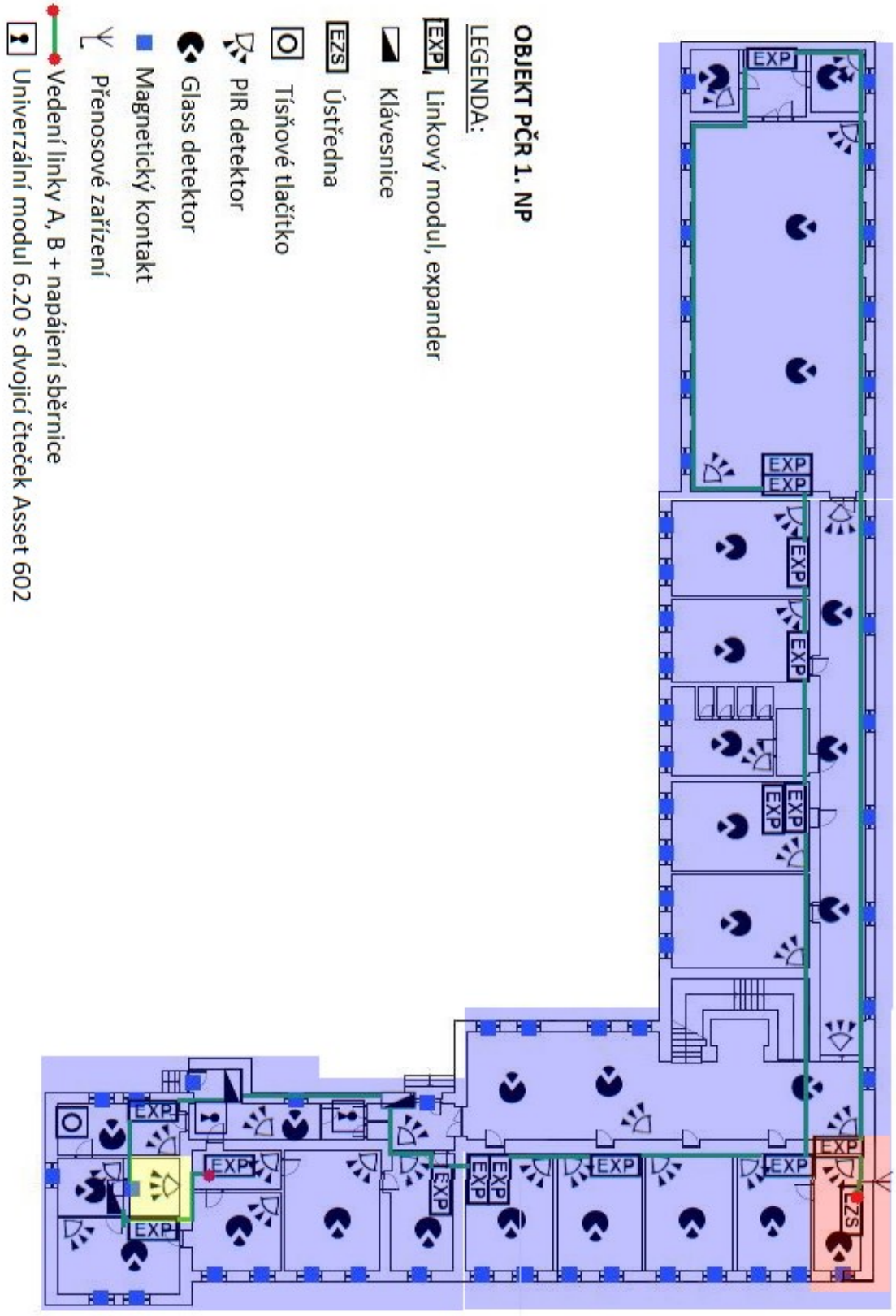
UTP Unshielded twisted pair, nestíněná kroucená dvojlinka

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: VYZNAČENÍ PODSYSTÉMŮ PŘÍZEMÍ



PŘÍLOHA P II: VYZNAČENÍ PODSYSTÉMŮ DRUHÉHO PODLAŽÍ