-

Zabezpečení s využitím grafických nadstavbových systémů

Vokurka Roman

Bakalářská práce
2019/2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Roman Vokurka**
Osobní číslo:	**A17269**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Zabezpečení s využitím grafických nadstavbových systémů**
Téma práce anglicky:	**Security with the Utilisation of Graphic Superstructure Systems**

Zásady pro vypracování

1. Proveďte rešerši o prvcích a systémech používaných pro grafické prostředí.
2. Popište základní prvky PZTS, SKV, EPS, DV a jejich zobrazování v grafickém prostředí.
3. Navrhněte zabezpečení objektu pomocí poplachových systémů.
4. Nakreslete schéma objektu a realizujte grafickou nástavbu celého systému.
5. Odhadněte další vývojové trendy v této oblasti.

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

Seznam doporučené literatury:

1. VALOUCH, Jan. Projektování integrovaných systémů. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2015, 1 online zdroj (169 s.). ISBN 9788074545573.
2. LUKÁŠ, Luděk a kolektiv. Bezpečnostní technologie, systémy a management III. Zlín: VeRBuM, 2013. ISBN 978-80-87500-35-4.
3. LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I*. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. ISBN 978-80-7318-889-4.
4. LAUCKÝ, Vladimír. *Speciální bezpečnostní technologie*. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 978-80-7318-762-0.
5. BRABEC, František. *Technologie detektivních činností*. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 978-80-7318-780-4.

Vedoucí bakalářské práce: **Ing. Rudolf Drga, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **7. prosince 2019**
Termín odevzdání bakalářské práce: **25. května 2020**

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Ve Zlíně dne 7. prosince 2019

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne …….

podpis diplomanta

ABSTRAKT

Bakalářská práce se zabývá seznámením laické veřejnost s moderními integračními zabezpečovacími systémy. Ukazuje, jakým způsobem se zpracovává navržená bezpečnostní instalace do moderního grafického softwaru sloužící k ochraně budov. Také seznamuje se zařízením, které je k tomuto účelu používáno a jaké mají vlastnosti.

Klíčová slova:

Integrační systém, grafické značky, zabezpečení, PZTS, CCTV, EPS, SKV.

ABSTRACT

This Bachelor thesis deals with acquaintingthegeneral public with modern integrationsecuritysystems. Itshowahowtheproposedsecurityinstallationisincorporatedintomoderngraphics software used to protectbuildings. Italsointroducestheequipmentthatisusedforthispurpose and whatitsproperties are.

Keywords:

Integration systém, graphic signs, security, PZTS, CCTV. EPS, SKV.

PODĚKOVÁNÍ

Tímto bych chtěl poděkovat všem, kteří mi byli nápomocni při získávání informací pro napsání této bakalářské práce. Také bych chtěl poděkovat mému vedoucímu práce panu Ing. Rudolfu Drgovi, Ph.D. za cenné rady a odborné vedení, které mi poskytoval během této práce.

OBSAH

ÚVOD

Dnešní doba je v mnoha ohledech odlišná vůči minulosti. Hrozby, které jsme doposud neznali či slyšeli o nich jen z doslechu se nyní prokazatelně objevují před naším prahem. Nutnost si chránit své zdraví, zdraví své rodiny, potažmo i svůj vlastní majetek je bohužel každým dnem naléhavější. Možností, jak toho docílit není, vzhledem k legislativě, málo. Jednu z nich je zabezpečení vlastního bydlení, firemního majetku apod. formou moderních technologií. Tato ochrana začíná již perimetrem chráněného objektu, pak pokračuje přes plášťovou ochranu a končí u předmětové ochrany. Veškeré tyto části ochrany mohou vhodnou volbou technologií chránit objekty vůči různým druhům útoku. [1;2;3;4]

I. TEORETICKÁ ČÁST

1 ZABEZPEČOVACÍ SYSTÉMY

Moderní doba s sebou přináší moderní technologie a pokrok v oborech, které mohou tento potenciál ve vývoji těchto technologií velice dobře využít. Požívání integrovaných systému grafické nadstavbě je horkým trendem posledních let. Firmy se začaly specializovat na tuto problematiku a přináší na trh každým rokem celou řadu hardwarového a softwarového vybavení určeného pro užití v zabezpečovací technice. Samotná podstata takového sytému tkví v užití základních zabezpečovacích prvků a využití jejich vlastností k přehlednějšímu a efektivnějšímu užití. Propojení veškerých systému do jednoho celku neboli centrálního uzlu pak umožňuje obsluze včasně reagovat na případný incident a korektně ho vyřešit. Z toho plyne, že hlavním cílem takového systému je maximální přehlednost, a tím zrychlení řešení vzniklých událostí. Propojení rozdílných systémů PZTS, SKV, EPS a CCTV na DPPC do jednotného celku je tedy požadavkem od zákazníka a směrem, jímž se ubírá dnešní trend vývoje. V další části si probereme jednotlivé segmenty, z kterých se skládá integrovaný systém převedený do grafického rozhraní.

1.1 Systém PZTS

První ze segmentů, který se podílí na integrovaném systému je poplachový tísňový a zabezpečovací sytém (PZTS). Jeho jádrem je ústředna PZTS, do níž jsou připojeny veškeré detektory potřebné pro zabezpečení daného objetu. Každá ústředna ať se jedná o ústředny PZTS, EPS, SKV má v útrobách akumulátor sloužící jako záložní zdroj pro případ pro případ náhlého výpadku elektřiny zajišťující funkčnost systému po tuto dobu. Zde si budeme zmiňovat pouze o nejběžnějších prvcích používané pro zabezpečení domácností a malých firem. Jsou to pasivní IR PIR detektory, magnetické kontakty, detektory rozbití skla, otřesové detektory, tísňová tlačítka a ovládací prvky, konkrétně klávesnice sloužící obsluze. Existují však spousty dalších detekčních prvků, například detekční kabel, IR závory, kapacitní detektory, mikrovlnné detektory apod.

Ústředna PZTS jak bylo uvedeno výše, je centrálním místem, kam jsou svedený všechny technologie PZTS. Její ovládání a potažmo ovládání celého systému je umožněno pomocí tlačítkové klávesnice. Za pomoci této klávesnice může uživatel ovládat proces střežení, případně administrovat celou ústřednu. Tato metoda administrace přes klávesnici není příliš uživatelsky příjemná, a proto lze využít, například u systémů ATS, programovací software TITAN, v němž lze administraci celého systému přehledně a velice rychle spravovat a manažerovat všechny uživatele s jejich právy a hesly.[5]

Obr. 1 Ukázka ústředny PZTS

Pro PZTS ústřednu se využívá jako symbol toto grafické znázornění: 

1.1.1 PIR detektor

Pasivní infračervený PIR detektor zaznamená narušení prostoru ve vymezené oblasti a následně tuto informaci předá do ústředny, čímž vyvolat poplach. Princip detekce spočívá v sledování teploty objektů v hlídaném sektoru. Pyroelektrický snímač v detektoru pracuje v oblasti infračerveného pásma, jenž odpovídá právě vyzařování tepla z lidského těla. Sektor je rozdělen podle typu PIR detektoru do několika zón. Takto rozdělený prostor na zóny pak hlídá změnu v teplotě mezi těmito zónami. Pokud se změní teplota mezi zónami v dostatečně rychlém čase, nastane procedura spuštění poplachu. Z toho si lze snadno odvodit, jaké jsou omezení v detekci. Pokud osoba bude stát a nebude zaznamenán přechod mezi zónami, nedojde k spuštění poplachu. Také se snižuje jeho schopnost detekce, pokud osoba se pohybuje směrem k detektoru, kde v tomto směru nepřesahuje mezi zónami detekce. Z principu detekce založeného na teplotě je problematická i teplota okolí, v kterém detektor pracuje. Pokud dochází k rychlejším výkyvům teploty muže dojít k nežádoucím falešným poplachům. Problém je i pří klesající teplotě. Při nízkých teplotách dochází k zhoršení detekci, není-li detektor určen pro venkovní užití. Jeho nevýhody však mohou být i výhodou. Například nedetekuje přes průhledné objekty, a proto nezaznamená

pohyb za okny. Proto lze instalaci detektoru zvážit, pokud není jiné možnosti i proti oknům a vyhnout se tím nežádoucím falešným poplachům způsobené pohybem objektů za okny. Další nepříjemné omezení je nemožnost rozlišování velikosti detekujících objektů. Nelze tedy rozlišit, zda jde o osobu nebo o domácí zvíře. V tomto případě lze u detektorů použít speciální čočky/clony, které omezují profil detekčního pole (charakteristiky) detektoru, a tím mohou odfiltrovat falešné poplachy způsobené například pohybem psa v místnosti. V dnešní době jsou již na trhu celé řada různých druhů detektorů, které kombinují více funkcí v jeden kompaktní celek. K detektorům jsou přidávané prvky, jako je antimasking zajišťující detekci před zakrytím detektoru nebo teplotní kompenzace snižující počet falešných oplachů z důvodu náhlé změny teploty apod. Detektory jsou již kvalitně spravovány a mají velice dobrou spolehlivost i dlouho životnost, například detektor s kamerou nebo detektor PIR kombinovaný s detektorem rozbití skla apod. Charakteristiky PIR detektoru, jenž je tvořen použitím různé soustavy čoček rozdělujeme do několika skupin. Na obrázku 2 je zachycen venkovní bezdrátový PIR detektor od firmy Jablotron typ JA-89P.

Obr. 2. PIR detektor

Detektory se rozdělují dle charakteristik do několika skupin

- se standardní charakteristikou
- s širokoúhlou charakteristikou
- s kruhovou charakteristikou
- s bariérovou charakteristikou
- s dlouhým dosahem
- PetAlley

Detektory dále rozdělujeme podle použité optické soustavy. Existují pouze dva druhy optiky, které se nejvíce u těchto pasivních PIR detektorů používají.

Používaná optika

- čočka
- lomená zrcátka

Čočková soustava používaná v IR pasivních detektorech je tvořena převážně z plastového materiálu z důvodu nižších výrobních nákladů a její nízké váhy oproti klasickým skleněným čočkám. Soustava je navržena tak, aby elektromagnetické vlnění procházející čočkou bylo ohnuto přímo do snímače detektoru, jinak řečeno: snímač detektoru je umístěn přímo v ohnisku čočky. Fresnelova čočka je nejpoužívanější plastovou čočkou u detektorů. Její hlavní výhodou je snížení nároků na výrobní materiál a nižší hmotnost vůči klasickým tvarům čoček, ať jsou vyrobeny z plastu nebo skla. To je dosaženo odejmutím materiálu z částí čočky, jež se nepodílí na lomu elektromagnetického vlnění. Technologie LOFID používaná v nové generaci těchto čoček dokáže pokrýt korektně všechny mrtvé úhly. I když tato čočka nedisponuje kvalitou klasických čoček, přesto je to nejpoužívanější součást v moderních PIR detektorech.

Pro PIR detektory se využívá jako symbol toto grafické znázornění: 

1.1.2 Otřesový detektor

Otřesový detektor (OTD) se využívá především při ochraně trezorů či místností, které jsou určeny pro stupeň vyhrazené – přísně tajné. Novější detektory jsou schopné i detekovat náklon hlídaného objektu. Nejdůležitější u OTD je jejich správná instalace, aby nedocházelo vlivem nedůsledného umístění k falešným detekcím případně, že by detektor vůbec nezaznamenával žádné vibrace. Také se při instalaci těchto detektorů musí brát v úvahu prostředí kolem detektoru, zda nejsou v jeho blízkosti možné zdroje nežádoucích otřesu například projíždějící tramvaje před budovou. Na obrázku níže jsou vyfoceny otřesové detektory OTD GM 730 a VV600PLUS s jejich vnitřním uspořádáním.[5]

Obr. 3. Otřesové detektory

Pro otřesové detektory se využívá jako symbol toto grafické znázornění: 

1.1.3 Magnetický kontakt

Spadá do oblasti elektromechanických detektorů. Hodí se k plášťové ochraně budov, například jako zabezpečení dveří a oken apod. Da se využít i k zabezpečení objektu proti odcizení obrazy nebo umělecká díla obecně před odcizením. Základem magnetického kontaktu jsou dva překrývající se jazýčkové kontakty umístěné a zatavené ve skleněné baňce, která je naplněna inertním plynem. Převážně tímto plynem je dusík, ale používá se k plnění i argon. Jazýčkové kontakty uvnitř baňky jsou vyrobeny z měkkého magnetického materiálu za účelem rychlého zmagnetizování. Jejich povrch je galvanicky upraven pro lepší vodivost například zlatem, platinou, stříbrem nebo wolframem. Díky materiálu, z kterých jsou kontakty vyrobeny, se při vložení do magnetického pole zmagnetizují a přitisknou k sobě.

Tím se vytvoří vodivý kontakt, který trvá jen do doby, než magnetické pole zmizí. Magnetické pole je u těchto detektorů tvořeno druhou částí detektoru a jde o dostatečné silný permanentní magnet. Nevýhoda těchto detektorů je v nutné kvalitní instalaci, která je závislá na vzdálenosti permanentního magnetu od skleněné baňky. Pro snížení možnosti překonání těchto detektorů se dávají například do pouzdra detektoru dva kontakty a jeden z nich přebírá funkci sabotážního kontaktu. Na obrázku 3 jsou zachyceny některé druhy magnetických kontaktů například od firmy Jablotron.JA-111M. [5]

Obr. 3. Magnetické kontakty

Pro magnetický kontakt se využívá jako symbol toto grafické znázornění 

1.1.4 **Detektor tříštění skla**

Akustické detektory GB (GlassBreake) jsou používané nejčastěji v plášťové ochraně. U chráněných objektů je nejčastějším vnikem do hlídaných prostor právě skleněná plocha (okna, výplně dveří). Z tohoto důvodu patří tyto detektory ke stěžejním prvkům v ochraně objektu.[5]

Detektory seřazujeme do několika skupin

Podle umístěný v ochranném pásmu

- Plášťová ochrana
- Předmětovou ochrana
- Perimetrická ochrana
- Prostorová ochrana

Dále můžeme akustické detektory seřadit podle detekce zdroje akustického signálu.

- Aktivní
- Pasivní

Aktivní – pachatel při svém konání překonává pole vytvořené detektorem a změny v tomto poli jsou následně detektorem zaznamenány. Tyto detektory jsou vybaveny jak vysílací, tak i přijímací elektronikou.

Pasivní – tyto detektory pouze detekují vzniklé akustické signály, například zvuk destrukce skleněné tabule, a nevytváří aktivně žádné pole.

A také je lze řadit dle jejich rozsahu pracovní frekvence

- Akustické
- Ultrazvukové

Akustické – jejich rozsah pracovní frekvence je v rozmezí slyšitelného zvuku. Rozsah této frekvence je od 16 Hz do 20KHz.

Ultrazvukové – tyto detektory mají pracovní frekvencí nad slyšitelným zvukem tedy v pásma nad 20KHz.

1.1.4.1 Akustické detektory

Účelem detektoru je snímat destrukci skleněných ploch v jeho dosahu prostřednictví charakteristické akustické tlakové vlny vzniklé z této destrukce. Tento akusticky projev je snímán pomocí piezoelektrického měnič, případně lze použít i mikrofon. Detekční dosah těchto detektorů sahá do vzdálenosti řádově 25 m. Nutností pro funkci detektoru je jeho pásmová propust, která je omezí pouze na kmitočtovém spektru, které odpovídá tříštěný skla. Vzhledem k této propusti jsou jedno pásmové detektory náchylné na falešné poplachy z důvodu snímání úzkého pásma kmitočtu. Falešný poplach může způsobit ruch z ulice,

projíždějící tramvajový vůz, blízké kontejnery na sklo, telefony apod. Proto byly na trh uvedeny pásmové detektory vybaveny zvukovými analyzátory snižující falešné poplachy. Analyzátor zhodnocuje stádium zvuku ze dvou časových úseků. První zhodnocení je počáteční destrukce, která vygeneruje impulz s nízkou frekvencí s krátkým trváním (90 dB). Dále následuje zhodnocení dopadu sklených částí na podlahu. Na následujícím obrázku jsou zachyceny akustické detektory.

Obr. 4. Akustické detektory tříštění skla

Pro GB se využívá jako symbol toto grafické znázornění: 

1.1.4.2 Ultrazvukové detektory

Jedná se o detektory, které pro svoji funkci detekce využívají fyzikálního principu frekvence zvaného Dopplerův jev. Detektory se vyrábějí s ultrazvukovými přijímači a vysílači pracujících na totožné pracovní frekvenci. Dopplerův jev popisuje příčiny a důsledky změny frekvence závislosti na rychlosti a vzájemné poloze zdroje signálu a pozorovatele tohoto signálu. Detektor vysílá ultrazvukový signál o definované frekvenci a přijímá její odraženou složku například od stěny zpět v hlídaném prostoru. K vyhlášení poplachu dojde v případě, že se vyslaná frekvence liší od přijaté. Na tomto principu pracují jak ultrazvukové, tak mikrovlnné hlásiče. V případě ultrazvukových hlásičů muže docházet problémům u zvířat. Protože pracují za hranicí slyšitelnosti pro lidské ucho, nedá se vyloučit, že tento zvuk nemůžou zachytit zvířata. Mou pak být vystaveni psychickému tlaku způsobeného

tímto zvukem. Detektory pracující na frekvenci ultrazvuku mají i určitá omezení související jejich umístění. Nesmí se instalovat v blízkosti zdrojů široko-kmitočtovým spektrem (u telefonu), neinstalují se nad topná tělesa či závěsy apod. Vše by totiž mohlo ovlivnit jejich detekční funkci.

1.2 Systém SKV

Centrem sytému SKV je řídící jednotka. Tato jednotka obsahuje veškeré údaje o celém systému ve své paměti EPROM, která v základu muže obsahovat až 13 000 záznamů o uživatelích. Jedná se o časové rámce a osoby, které mají povolený vstup na patřičné přístupové body. Stěžejní součástí SKV je čtecí hlava, která umožňuje načíst údaje čipové karty v kterých je ukryt malí RF čip a pracuje na frekvenci například 126 KHz. Načtením přístupové karty na čtecí hlavě se autorizuje přístupové oprávnění přiřazené této kartě potažmo vlastníkovy této karty. Pro možnost autorizace v SKV systému se používá celá škála různých tokenů, jako jsou přívěsky na klíče, prsteny, náramky, krabička pod nárazníkem auta apod. Všechny tyto tokeny mají jedno společné. Fungují na principu RF technologií, tedy bezdotykového přístupu. Další možností autorizace je například magnetické pásky nebo použití biometriky, např. bio čtečky, snímače obličeje, otisk prstu či sítnice a vše je možné doplnit o pinovou klávesnici. Administrace řídících jednotek probíhá prostřednictvím serverů používající patřičný softwarový program jako například program GRANTA. S pomocí těchto programů je administrace uživatelů pro operátory velice rychlá a přehledná. Lze například vytvořit díky tomu snadný a pohodlný docházkový systém či přehledný soubor přístupových oprávnění a časových rámců pro firemní potřebu. V čtecí hlavě nalezneme anténu, která zprostředkovává komunikaci a načítaným tokenem. Samotné generování vysílaní a příjmení má na starosti RF modul uvnitř řídící jednotky a ovládání elektrických zámku se provádí spínáním relé na základní desce samotné řídící jednotky. Systém také muže disponovat pinovou klávesnicí či odchodovým tlačítkem a dalším příslušenstvím. Na obrázku níže je zachycena řídící jednotka s instalovaným RF modelem a jedním modulem pro dveřní systém s jednou čtecí hlavou.[5]

Obr. 5 Řídící ústředna SKV osazená prvky

Pro SKV řídící jednotku se využívá jako symbol toto grafické znázornění 

Pro čtecí hlavu se využívá jako symbol toto grafické znázornění 

Pro čtecí hlavu s PIN se využívá jako symbol toto grafické znázornění 

Pro znázornění dveří se využívá jako symbol toto grafické znázornění 

1.3 Systém CCTV

Systém uzavřeného kamerového systému (Close Circuit Television) je k vidění v dnešní době téměř na každém našem kroku. Veškerá obchodní centra, rušné křižovatky, dálnice či úřady a další objekty jsou tímto systémem vybaveny. V dnešní době jde o jeden z nejpoužívanějších nasazovaných prvků v oblasti ochrany. Tyto prvky nám vhodnou formou dokáží zvýšit bezpečnost, a pokud jsou umístěny na viditelném místě tak mají i preventivní charakter. Hlavní součástí dnešních systému tvoří kamerová zařízení, která jsou propojeny s nahrávacím a vyhodnocovacím zařízením, které obsluhuje operátor a za pomoci zobrazovacího aparátu vyhodnocuje zaznamenané skutečnosti. Záznamy z kamer jsou zálohovány po určitou dobu pro případné dohledání vzniklých skutků k účelu řešení Policií České republiky.[5]

1.3.1 Kamery

Jsou hlavní částí kamerového systému. Postupem času se kamery vyvíjeli z analogových přes barevné až k dnešním digitálním zařízením. Převádějí optickou zaměřenou scénu na obrazy monitorů.

Kamery rozdělujeme do tří skupin na:

- Analogové kamery
- Digitální kamery
- IP kamery

Analogové kamery

Analogové kamery převádí obraz na elektrický signál pomocí světlo citlivého snímače a k přenosu se používá formát rozlišení PAL (720 x 576 při 25 FPS) nebo NTSC (720 x 480 při 30 FPS) či SECAM (525 řádků). Tedy signál vyvedený z této kamery má analogovou formu. Z kamery je veden prostřednictvím konektoru (cinch, BNC) za pomoci koaxiálního kabelu například do videorekordéru (DVR) do kterého jsou připojeny sledovací monitory pro obsluhu. Pokud je nutno rozdělit signál z kamery na více zařízení, využívají se k tomuto účelu kvadrátory nebo multiplex éry a podobná zařízení, která nedisponují možnosti ukládaní záznamu. Vzdálenosti mezi kamerou a DVR je závislá na použitém typu kabelu. Pro koaxiální kabely, kroucené dvojlinky nebo rádiové kanály jsou vzdálenosti pouze v řádů několika stovek metru (pro koaxiální kabel přibližně 100 m). Ale při použití vhodných převodníků a kabeláže (optické vlákno, IR přenos případně rádiová pojítka) můžeme dosáhnout vzdálenosti i několika kilometrů. Tyto kamery jsou v dnešní době velice rychle nahrazovány digitální kamerou, vzhledem k velice malému rozlišení a velice špatné kvality obrazu. Rozlišení je udáváno pro analogové kamery v TVL což je horizontální rozlišení obrazu. Například kamera s hodnotou 800 TVL má rozlišení 800 x 600. V důsledku používaných omezujících formátu u analogových kamer jako jsou, PAL a NTSC větší rozlišení kamery neznamená automaticky kvalitnější obraz. Na obrázku 6 je vyfotografována analogová kamera s detailem fotocitlivého prvku (CCD čip).

Obr. 6. Analogová Kamera s CCD

Pro kameru se využívá jako symbol toto grafické znázornění: 

Pro otočnou kameru se využívá jako symbol toto grafické znázornění: 

Digitální kamera

Digitální kamery již přenášejí obraz v celku, a ne po řádcích, jak tomu je analogového přenosu. Velikost obrazu se udává v megapixelech (1 MPx je rozlišení P720, tedy 1280 x 720 obrazových bodů). Signál je již číslicový a je tedy mnohem odolnější vůči vlivům ručení, než má analogový signál. Díky vlastnostem takového systému je rozlišení u digitálních kamer takřka neomezené. Kvalita přenášeného obrazu je závislá pouze na přenosové schopnosti používané sítě, pro svou funkčnost používají normální protokol TCP/IP a lze je využívat i v síti ethernetu. O kvalitní zaostření a úpravu snímaného obrazu se starají elektronicky součástky zvané CCD (Charge –CoupleDevice). Jde o zařízení pracující na bázi vázání nábojů. V základu této technologie jde o to, že dopadající foton na fotodiodu vyvolá elektrické napětí, které se změří a velikost napětí určuje intenzitu jasu. Kvalita obrazu je závislá na převedených bodech prostřednictvím CCD. Čím je bodů více tím je obraz ostřejší a kvalitnější a naopak. Dnes se používají technologie nábojově vázaných prvků CCD a technologie unipolárních tranzistorů CMOS čipů. U obou těchto technologií zůstává světlo citlivým prvkem fotodioda vyrobena z křemíku.

Digitální kamery se rozdělují do dvou skupin dle počtu CCD

- kamery s jedním CCD
- kamery s třemi CCD

Hlavním rozdílem je v kvalitě zobrazení. Jednočipové kamery nemají takové dispozice na kvalitu obrazu jako tříčipové. U tříčipových kamer se obraz zachycený objektivem rozloží do základních tří barev světla (Red, Green, Blue), které samostatně procházejí barevnými

filtry kamery, po kterých jsou zachyceny třemi CCD prvky. Toto umožní elektronice kamery zpracovat jednotlivé složky odděleně a z této procedury vzniklý signál z těchto složek tvoří celistvý, velice kvalitní zobrazení.

Další nedílnou součástí kamery jsou odnímatelné (vyměnitelné) objektivy. Přes něj je snímaná scéna promítána na fotocitlivé součástky uvnitř kamery (CCD čip). Dokáže upravovat světlost scény a celou řadu optických podmínek. Důležité parametry objektivu jsou ohniskové vzdálenosti, clony, hloubka ostrosti, čí způsob přichycení ke kameře.

IP kamery

Je to trend dnešní doby. Jde o vylepšenou verzi digitálních kamer v rámci síťového přenosu dat. Samotné kamery jsou vybaleny například konektory RJ 45 pro připojení do Ethernetu. Požitím technologie PoE (PoweroverEthernet) switche propojení kamery za pomoci UTP kabelu odpadá nutnost při instalaci vést více kabelu, případně hledat možnosti odkud kameru napájet. Také tyto kamery disponují i logickým výstupem a vstupem a lze je propojit se systémy jako je PZTS.

1.4 Systém EPS

Podobně jak je tomu u systému PZTS i EPS má své hlavní centrum v ústředně. Rozhodovací postupu jsou prováděny právě zde. Do této ústředny jsou svedeny veškeré požární hlásiče pomocí smyček, což není nic jiného než kabelové vedení propojující veškeré hlásiče. Ústředna je vybavená vlastní malou jehličkovou tiskárnou tisknoucí na termopapír, která zaznamenává veškeré události v systému pro případ zpětného dohledání událostí. Systém detekce požáru je dán adresací hlásičů nebo smyček. Pokud máme na mysli systém určující pouze adresaci na smyčce, jedná se o systém s kolektivní adresací. Tento systém pouze vyhodnotí, na které ze smyček vznikl poplach požáru, ale již nám nesdělí přesnou lokaci požáru. Jinak řečeno přímo nezjistíme, který hlásič na smyčce tento poplach vyvolal. Pokud se jedná o systém s individuální adresací, má v tomto systému každý hlásič svou jedinečnou adresu a díky tomu lze ihned zjistit, který hlásič poplach vyvolal. Tento systém se používá u všechvětších instalací, kvůli rychlé lokaci možného požáru a tím ochránit ujmu na zdraví či poškození majetku.[6]

Rozdělení hlásičů požáru

- Tlačítkové:
  - 1) přímá obsluhou
  - 2) nepřímá obsluhou
- Hlásiče samočinné

1.4.1 Tlačítkové hlásiče požáru

Přímá obsluha:

U tohoto typu hlásiče pro jeho aktivaci je nutné, aby obsluhou rozbila skleněné sklíčko, pod nímž je ukryt spouštěcí mikrospínač, případně existuje i možnost odsunutí tohoto sklíčka stranou a tím se tento mikrospínač sepne.

Nepřímá obsluha:

Pro aktivaci požárního poplachu je nutné rozbít či posunout sklíčko, jak je tomu v předchozím případě, ale ještě je nutné, aby obsluha stiskla tlačítko pro vyvolání požárního poplachu.

Po aktivaci požárního hlásiče ať s přímou nebo nepřímou obsluhou zůstávají aretovány v poloze požárního poplachu. To je docíleno použitím magnetické, převážné však

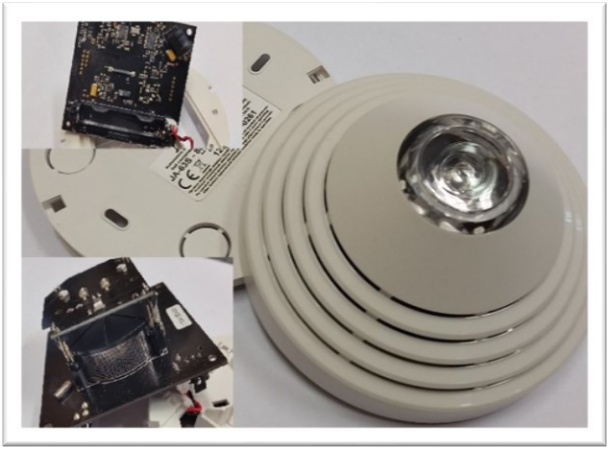
mechanickou aretace. Proto nelze takové hlásiče na dálku uvést do původního stavu. Do předešlého stavu je nutno tyto hlásiče resetovat přímo na místě za pomoci dodaných přípravků od firmy spolu s výměnou poničeného sklíčka či zpětným zasunutím sklíčka do původní polohy.

1.4.2 Samočinné hlásiče

Samočinné hlásiče jsou bezesporu tou nejlepší možnou formou ochrany majetku a zdraví lidí před požárem. Dokáží nepřetržitě hlídat možné vzniky ohnisek požáru, na která by se mohlo přijít pozdě v případě spoléhání pouze na lidský faktor.

Dělení samočinných hlásičů

- Kouřové hlásiče – rozdělujeme na hlásiče
  - Ionizační hlásiče
  - Optické hlásiče
- Teplotní hlásiče
- Multifunkční hlásiče
- Hlásiče plynu
- Hlásiče plamene



Obr. 7. Kouřový optický hlásič

Pro EPS ústřednu se využívá jako symbol toto grafické znázornění

Pro hlásiče požáru se využívá jako symbol toto grafické znázornění

Pro tlačítkové hlásiče se využívá jako symbolu toto grafické znázornění

Vodivost plynu

Plyny jsou velice dobrým izolantem za normálních podmínek, protože jsou téměř nevodivé. To je zapříčiněno velice malým množstvím iontů v jejich objemu a stanou se vodivými pouze v případě, pokud nastanou k tomu vhodné podmínky. Z toho plyne, že pokud budeme chtít z plynu udělat vodič, stačí do jeho objemu přidat dostatečné množství iontů. Problém v tomto směru nastává v neustálém dotování iontů do plynu, jinak se z něj stává opět izolant. Důvodem je fyzikální vlastnost iontů v plynech. Ty se při setkání s opačnou částicí mění na neutrální, a tím se neutralizují. Možností, jak dosáhnout ionizace plynu je několik. Hlavním cílem je vždy odtržení elektronu z vazby od atomu. Tou první je vysoká teplota, kde molekuly mají již dostatečnou energii a během srážek se odtrhávají z vazeb elektrony, čímž dochází k ionizaci plynu. Druhá možnost, jak docílit ionizaci plynu je použití elektrického pole. Tato metoda je založena na urychlení již iontů v plynu obsažených. Díky elektrickému poli tyto ionty se urychlit na dostatečnou rychlost, která dostačuje k tomu, aby při srážce s molekulou plynu odrhla z vazby nějaký elektron. Třetí množností je radioaktivní záření α, β částic. Podobný princip jako u elektrického pole. Tyto částice mají velmi vysokou rychlost a dokážou při srážce s molekulou odtrhávat elektrony a ionizovat tímto plyn. Poslední možnou metodou je elektromagnetické záření. Ionty v tomto případě dokážou získat dostatečnou energii pro odtržení od jádra atomu pohlcením záření paprsků X případně γ.

1.4.2.1 Ionizační kouřové hlásiče

U těchto hlásičů probíhá detekce na základě vyhodnocení rozdílu ve vodivosti ionizačního plynného prostředí. V těle hlásiče je umístěna detekční komůrka, přes kterou prochází plyn a jeho následnou analýzou obsahu nezoxidovaných pevných částic kouře v komůrce vyhlásí při určeném množství poplach.

1.4.2.2 Optické kouřové hlásiče

Oproti ionizačním hlásičům optické hlásiče detekují poplach prostřednictvím změny v šíření světelného paprsku. Během hoření se do prostoru, kde je hlásič umístěn uvolňují pevné částice tímto ohněm generované. Částice se postupem času dostanou do vnitřních částí hlásiče. V něm ovlivní šíření emitovaného světelného paprsku. Ten je umístěn v komůrce, kde za normálních podmínek prochází vrstvou vzduchu a není nijak ovlivněn.

Vniklé částice z hoření se dostanou do tohoto prostoru a způsobem dle typu hlásiče pak dojde k vyvolání poplach.

Optické kouřové hlásiče se rozdělují do dvou skupin dle procedury vyhodnocení poplachu.

a) Vyhodnocení na základě rozptylu emitovaného optického paprsku
b) Vyhodnocení na základě absorpce emitovaného optického paprsku

Rozptyl

Hlásiče požáru na principu rozptylu emitovaného světelného paprsku jsou převážně vybaveny generováním tohoto paprsku za pomocí infračervené LED diody. Vnitřní část hlásiče je tvořen komůrkou, která je speciálně navržena, aby nepropouštěla do vnitra světlo pomocí soustavy lamel a zároveň jí bezproblémově proudil vzduch, potažmo kouř způsobený požárem. Detekce požáru pak proboha v této tmavé části hlásiče. Součástí detekční komůrky je přijímač i vysílač světelného paprsku usazeny záměrně v takové konfiguraci, že se za normálních podmínek nevidí. Znamenáte, že světelný paprsek nedopadá na detekční plochu přijímače. K rozptylu světelného paprsku dojde v okamžiku interakce pevných částic generovaných kouřem proudících u vnitřních prostor komůrky, a to zapříčiní dopad tohoto paprsku na detektor.

Absorpce

Hlásiče pracují na principu pohlcování emitovaného paprsku a vyhodnocení této změny. Jsou zhotoveny ze dvou navzájem oddělených částí. Základem hlásiče jsou dva prvky, a to přijímač a vysílač. Používáním tohoto způsobu detekce lze pomocí velikostí vlnové délky detekovat různě velké kouřové pevné částice řádově od 0,1 až 10 μm. Existují dva způsoby konstrukce tohoto provedení. Buď to jsou tyto dva prvky navzájem od sebe odděleny, nebo můžou být dány do jednoho pouzdra a součástí tohoto provedení je zrcátko sloužící k odrazu emitovaného paprsku z vysílače do přijímače. Přijímač není ničím jiným než fotodetektor reagující na dopadající infračervené záření emitováno z vysílače. Z konstrukčního hlediska se tyto hlásiče proto nazývají lineární. Vlastností infračerveného křemíkového přijímače spočívá ve výrobě elektrické energie, pokud na něj dopadá IR záření. Toto vznikající napětí odpovídá intenzitě dopadajícího záření na fotodetektor. Další částí hlásiče je kolimační optický systém. Tímto se intenzita dopadajícího záření snadno nastavuje prahová citlivost detektoru vhodnou formou po procentech. V důsledku použití IR takto koncepčně vytvořeného hlásiče lze používat tento druh hlásiče na velkou vzdálenost až 100 metrů.

1.4.2.3 Teplotní hlásič požáru

Jedná se o jeden z prvních prokazatelně nejstarších používaných hlásičů požáru. Vývoj těchto hlásičů se datuje již od roku 1860. Samotná detekce těchto hlásičů je založena na teplotních změnách v oblasti instalace. Teplotní změny jsou vyvolány uvolněním tepla z hoření tedy exotermickou reakcí. Vzhledem ke vlastnostem šíření tepla (konvekce) v plynném prostředí prouděním dochází po čase k tepelným změnám na senzoru hlásiče a vyvolání poplachu.

Teplotní hlásiče se rozdělují do dvou skupin:

- Lineární hlásiče
- Bodové hlásiče

Bodové hlásiče

Jádrem detekce u těchto hlásičů je převážně termistor kontrolující změnu teploty. Hlídá se změna v překročení nastavené teplotě nebo rychlost změny teploty. Poplach je vyvolán okamžitě, pokud dojde u jednoho z parametru, případně obou, k překročení těchto nadefinovaných hodnot. Starší diferenciální hlásiče dokázali vyhodnocovat také objemové a tlakové rozdíly při odlišných teplotách v hlídaném prostoru.

Lineární hlásiče

Tento druh hlásiče detekuje požár prostřednictvím modulační frekvence infračerveného vysílače. Na přijímač dopadá IR paprsek z vysílače, který prochází skrze střežený prostor a přijímač následně vyhodnocuje jakékoli změny. Pokud v hlídaném prostředí nastanou nějaké změny odlišné od normálního stavu, například nastane turbulentní proudění vzduchu s rozdílnou teplotou, dochází tímto vlivem na hranicích těchto rozdílných prostředí ke změně indexu lomu a parsek, který dopadne na přijímač má rozdílnou charakteristiku než předtím.

Teplotní liniově lineární hlásiče

Tyto hlásiče jsou podobné svým vzezřením klasickým kabelům. Jejich detekční prvky jsou tvořeny z teplocitlivého druhu materiálu, který reaguje na teplotu. Podle použití materiálu lze rozdělit tyto hlásiče na tři skupiny.

1) Hlásič s metalickým detekčním kabelem
    - analogové
    - digitální
2) Hlásič s optickým detekčním kabelem
3) Hlásič s pneumatickým detekčním kabelem

Digitální hlásiče

Digitální hlásiče využívají jednoduchého principu skokové změny odporu v měřeném kabelu v důsledku poškození tohoto kabelu a tím následně vzniklého zkratu. V kabelu se ukrývají dva ocelové vodiče, které jsou vzájemně skroucené, jak je tomu vidět u telefonní kabeláže a zároveň jsou vodiče předpružené. Polymer citlivý na změnu teploty tvoří mezi těmito dvěma vodiči izolační vrstvu. Zbytek vrstev kabelu tvoří ochranná folie a svrchní plášť. Principem detekce požáru tohoto hlásiče spočívá v polymeru, který v důsledku tepla zničí (mechanicky) a dojde k poruše izolační vrstvy mezi vodiči. Následkem je pak vzniklý zkrat při dotyku obou neodizolovaných částí vodičů uvnitř kabelu.

Analogové hlásiče

Analogové hlásiče takřka naprosto podobné digitálním hlásičům. Rozdílem je použitý materiál na odizolování vodičů. Použitý materiál při zvýšení teploty mění své vlastnosti a stává se dle teploty částečně vodivým. Tedy vzniká jakýsi falešný zkrat. Na rozdíl od digitálních hlásičů po ukončení zdroje tepla se izolační materiál vrací do normálního stavu a je tedy ho možné nadále používat. U digitálních hlásičů při vzniku poplachu dochází k porušení izolační vrstvy, což je nevratný stav a je nutné část tohoto kabelu vyměnit.

Optický detekční kabel

U optického detekční kabelu modernějších variant se pro detekci využívá Ramanova rozptylu. Starší druhy hlásičů detektovaly změny optických vlastností světlovodu vyvolané tepelnými účinky, způsobené mechanickým namáháním. Principem těchto hlásičů byl světlovod pevně svázaný s válečkem za pomoci například aramidového vlákna, jenž svazoval obě části pevně k sobě. Samotný váleček byl tvořený z hodně rozpínavého

materiálu. Při zvyšující se teplotě se objem válečku zvětšoval a světlovod, který byl pevně mechanicky přivázán k tomuto válečku se začal vlivem rozpínání „škrtit“. Tím se začal světlovod pozvolna deformovat a ovlivňovat optické vlastnosti, které byli sledovány a vyhodnocovány. U novějších, jak je již zmíněno, se využívá Ramanova rozptylu. Jde o využití vlastnosti světla, kdy při interakci fotonů s vibrujícími atomy případně molekulami, dojde ke změně vlnové délky záření. Rozdíl mezí dopadajícím a odraženým zářením se následně vyhodnocuje a pokud je rozdíl dostatečný, je vyvolám poplach. Hlásič má schopnost z výsledků určit v jaké části se teplota zvýšila, adokonce i o kolik stupňů.

Pneumatický hlásič liniového typu

Principem hlásiče je detekce na základě sledování rozdílného tlaku, který je důsledkem zvýšení teploty a využitím tepelné roztažnosti plynů. Rostoucí teplotazvětší objem plynu uvnitř trubicového senzoru (až 130m délky). Celá soustava je zcela uzavřená a důsledkem objemové roztažnosti uvnitř ní se začne zvyšovat i tlak. Senzorem je dlouhá dutá trubička, která se tlakuje. Senzory systému po celou dobu nepřetržitě sledují změnu tlaku v soustavě. Z tohoto důvody se dá říci, že hlásič pracuje diferenciálně, kdy hlídá změnu teploty v čase, a staticky, kdy hlídá překročení nadefinované průměrné teploty. Součástí tohoto systému je malý kompresor udržující tlak v systému. Z důvodu zvýšeného tlaku v systému je nutné zajistit jeho celistvost před možným únikem tlaku ze soustavy. Pro tento případ je systém vybaven procedurami k zjišťování úniku tlaku ze systému. Procedury spočívají v periodickém přetlakování soustavy za běžného provozu a měření doby poklesu tlaku v soustavě. Jakákoliv zjištěná závada na systému je pak vyhodnocena jako porucha.

1.4.2.4 Hlásiče plamene

Dle konfigurace se tyto hlásiče řadíjako bodové. Jejich funkce spočívá v detekci radiace vznikající prostřednictvím plamene. Tato vzniklá radiace má specifické vlastnosti, která se může spolehlivě detekovat. Mezi snímané detekční vlastnosti plamene spadá spektrální charakter vyzařování, oscilace plamene či intenzita vyzařování. Lze též tyto hlásiče řadit i k těm nejrychlejším hlásičům v oblasti detekce vzniku požáru. Z důvodu možnosti detekovat různá spektra záření se rozdělují do tří skupin.

1) Hlásiče plamene porcující v oblasti infračerveného záření (IR)
2) Hlásiče plamene pracující v oblasti ultrafialového záření (UV)
3) Hlásiče plamene pracující v oblasti jak infračerveném, tak ultrafialovém záření

IR hlásič plamene

Hlásiče plamene pracující v oblasti IR jsou vybaveny optikou, která je uzpůsobenák propuštění jen IR spektra ze záření plamene a současně je hlásič s touto optikou schopen odfiltrovat rušivé složky ovlivňující detekci hlásiče jako je sluneční svit apod. Základem těchto hlásičů jsou fotoelektrické nebo fotoodporové detektory vyráběné nejčastěji z křemíku případně sulfidu olova z důvodu levné výroby. Ale existují i detektory vyrobené z materiálu jako ‚arzen india' nebo ze ‚selenidu olovnatého'.

UV hlásič plamene

Hlásiče plamene pracující v oblasti UV využívají pro detekci emise OH radikálů, které vyhodnocují. Mají podobný princip algoritmu vyhodnocování jako IR hlásiče. Vyhodnocuje se velikost intenzity vyzařování ze vzniklého plamene. Podobně jako je tomu u IR hlásičů plamene se pro detekci používají fotoelektrické případně fotoodporové detektory vyrobené z karbidů křemíku nebo nitridu hliníku.

Poslední možností je i spojení obou těchto technologií do jednoho celku. Dostaneme hlásič, který detekuje vzniklý plamen jak v ultrafialovém spektru, tak v infračerveném. Takovýto hlásič detekuje požár ve dvou vlnových spektrech jak v UV, tak v IR.

1.4.3 Samočinné zhášecí systémy

Tyto systémy nepatří k hlásičům požáru, ale k prostředkům jak požár rychle a afektivně uhasit nebo ho alespoň dostat pod kontrolu. Systém je ovládán pomocí centrální jednotky EPS, která když vyhodnotí poplach z hlásiče za adekvátní, spustí proceduru hašení. Sytém EPS ústředny musí nejprve projít časovou osou odpočtu zvaných T1 a T2 před tím, než je vyhlášen poplach. T1 je čas kdy byl zaznamenán poplach a je nutné obsluhou fyzicky za pomocí ovládacího prvku, nejčastěji klíčku, přepnout na ústředně EPS čas z T1 do času T2.Tato doba je majoritně stanovena na 10 s od vyhlášení poplachu. Pokud to obsluha z nějakého důvodu nestihne přejde systém do času T2 s časem odpočtu 0 s, a tím vyhlásí systém rovnou poplach. Po přepnutí na T2 se spustí odpočet, který je dle obsáhlosti objektu různě dlouhý většinou kolem 10 minut. Za tu dobu má povinnost obsluha zjistit, zda jde o skutečny požár či nikoli. Pokud obsluha do této doby nevypne odpočet času T2, spustí se automaticky režim k opuštění budovy a pokud je systém vybaven samočinným systémem

zhášení tak ho aktivuje. Systém se také muže aktivovat okamžitě bez čekání spuštěním požárního tlačítka.

Média používaná pro hašení:

- voda – rozdělujese podle velikosti kapek
  I. Aerosol
  II. Vodní mlha
  III. Vodní tříšť
- plyn
- pěna
- prášek
- kombinované

Na obrázku níže je k vidění celí samočinný zhášecí systém s nádobami obsahující médium, požární jednotku, vedení média a ventily. Požární jednotka je napojena na požární hlásiče.

Obr. 8 Ukázka samočinného zhášecího systém.

2 GRAFICKÉ PROSTŘEDÍ

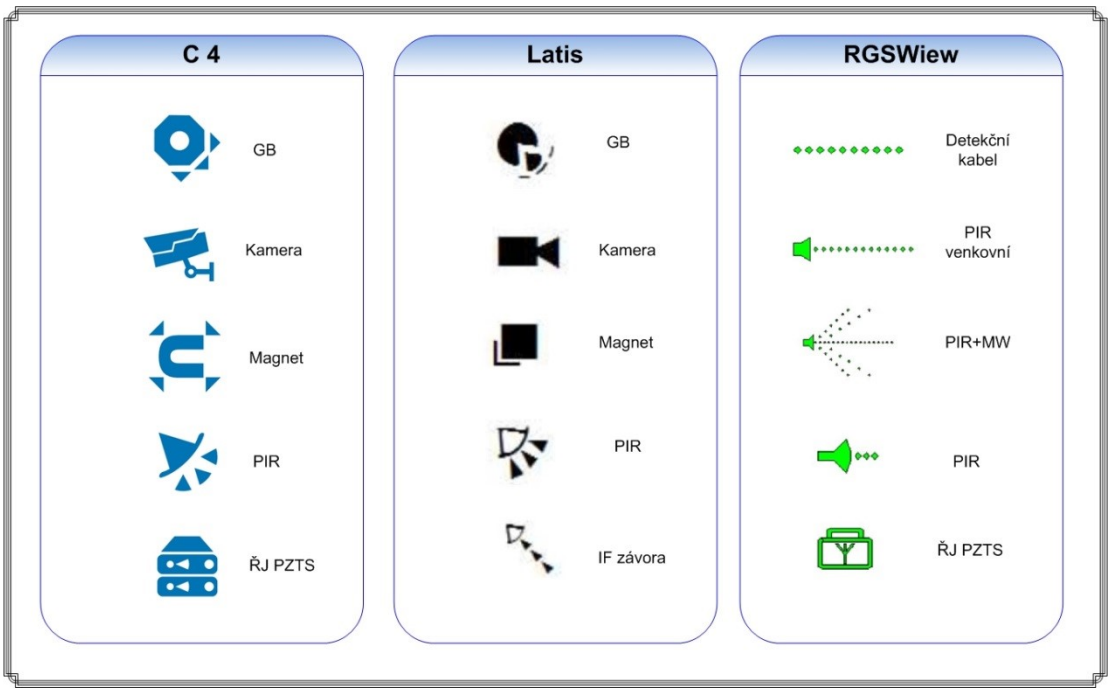
V nedávné doby každý zabezpečovací systém pracoval zcela autonomně. To s sebou neslo vetší nároky na obsluhu – na soustředění, na zajištění kvalitního dohled nad chráněnou oblastí. Pokrok v tomto směru se objevil v integraci bezpečnostních systémů do nadstavbového prostředí využívající grafickou vizualizace zabezpečovacích prvků. Prostřednictvím nových integračních nástrojů slučující systémy bylo docíleno bezpečnějšího zabezpečení jako celku. Dnes jsou na trhu celá řada softwarů, které tuto integraci dokáží vhodným způsobem zpracovat. Základem každé takového integrace je server, do kterého jsou svedeny veškeré technologie určené pro integraci. Proto je také důležité při projektování takového systému dbát na správné parametry tohoto stěžejního hardwaru, aby nedošlo v pozdějších etapách vývoje k problémům z nedostačující výkonosti právě tohoto zařízení. Je tím myšlena zejména nová softwarová úprava použitého softwaru (update). Nové verze jsou, zpravidla na hardware, mnohem náročnější než předešlé verze, ale z druhé strany přináší uživateli nové možnosti a vylepšení užívaného produktu. Pokud vlivem nové verze hardware dojde k hranicím jeho výkonu, nutně nastává pro celou infrastrukturu přirozený problém. Cely systém se začne zpomalovat a operátoři dostávají velice zkreslené informace o událostech na hlídaných objektech. Muže nastat až taková situace, že dojde ke kolapsu celého systému a nelze již hlídaný objekt dálkové monitorovat. Nemalou pozornost je třeba věnovat také velkosti uložiště dat v těchto serverech. Integrační softwary rádi ukládají velké objemy dat zvaných logy. Tyto logy jsou informace o veškerých událostech, které se dějí v celém systému. Jsou ukládány z důvodu zpětné kontroly případně k dohledání určitých poplachových událostí. Z toho plyne, že logy jsou informace například o průchodech v SKV systému nebo o činnosti PZTS systému apod. Nesmí dojít k situaci, že by v systému nemohl v důsledku nedostatečného prostoru dále software logy ukládat. Znamenalo by to ztrátu dat případně neuložení probíhajících aktuálních údajů ze systému. Tedy hlavním jádrem je server, na kterém běží integrační software. Jeho schopností je graficky znázornit pro obsluhu aktuální dění na hlídaném objektu. Zobrazení stavu systémů a detekčních prvků je u každého softwaru provedeno jinou formou. Společnou vlastností u těchto softwarů je mapový podklad. Na něm jsou umístěny formu aktivních ikonek prvky zastupující detekční, kamerové zařízení či jiné prvky. Pro názornou představu jsou na obrázcích níže zobrazeny ukázky grafického znázornění mapových podkladů ze dvou softwarů, a to Latis a C4, kde je znázorněn grafic-

ky systém PZTS. Obdobně jsou znázorněny i ostatní systémy jako EPS pouze prvkům jsou přiřazeny odpovídající značky znázorňující jejich podstatu.

Obr. 9. Mapový podklad v Latis pro PZTS upraveno z [7]

Obr. 10. Mapový podklad v C4 pro PZTS

Z bližšího prozkoumání předchozích podkladů vyplývá, že jsou systémy v této oblasti velice podobné. Principiálně grafická znázornění a funkce pro nastalé události si jsou také podobné. Znázornění poplachů, poruch, zastřežení zón a podobně jsou takřka identické. Odlišnosti v použitých symbolech nám však nebrání jejich vzájemné identifikaci, protože se používají standardně zažité značky v této oblasti s menším grafickým rozdílem. Na dalším obrázku jsou znázorněny vybrané grafické prvky a jejich symboly, které jsou užité v těchto softwarech a přidán k porovnání i jeden starší software RgsWeiw (2005) disponující pouze několika značkami prvků.



Obr. 11. Přehled grafických značek v softwarech C4, Latis, RGSWiew

Pomocí grafických značek je vždy možné rychle určit podle jejího symbolu, o jaký prvek se jedná. Všechny systémy CCTV, EPS, PZTS, SKV mají v softwarech předefinované značky, které se přiřazují k jednotlivým prvkům odpovídající jejich charakteristice. Tento krok svazující určitý prvek s danou grafickou značkou se děje za pomoci adresy. U všech softwarů používající grafické zobrazení je to stejný princip. Každý prvek, který je v systému, ať se jedná o samostatný systém nebo o integrovaný systém má vždy definovanou svou jedinečnou adresu, aby jej bylo vždy možné určit. K adrese daného prvku jako třeba kamera, PIR detektor či požární hlásič, se pak zvolí a naváže odpovídající grafická značka ze seznamu poskytnutým užitým softwarem. Takto svázaná značka s adresou odpovídajícího prvku pak definuje prvek v systému grafickým znázorněním,

například v mapách objektů a podobně. Díky tomuto postupu jsou se značkou svázány i stavy zastupujícího prvku jako je vyvolání poplachu, poruchy, stav off-line a další.[7]

II. PRAKTICKÁ ČÁST

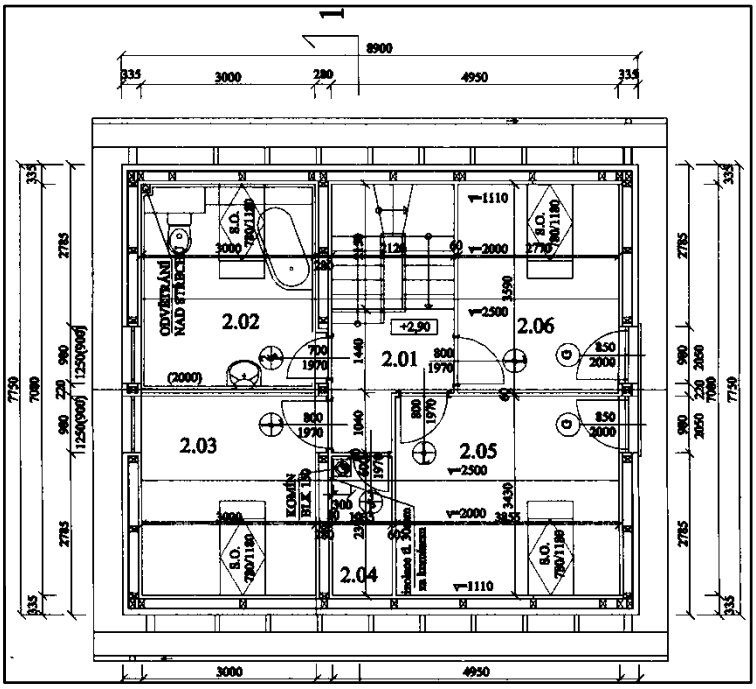
3 PLÁNOVÁNÍ ZABEZPEČNÍ

Prvním krokem v projektu zabezpečení je určení, o jaký objekt se jedná, kde je tento objekt situován a do jaké míry se bude muset chránit vzhledem k možným rizikům. Vhodná volba prvků ušetří investiční náklady a zároveň poskytne dostatečnou ochranu majetku, případně zdraví lidí. V našem případě však půjde o běžnou zástavbu – modelový dvoupatrový rodinný dům. V této souvislosti je předem dáno, že nepůjde o zvlášť hlídaný objekt s vysokým stupněm zabezpečení. Pro jednoduchost je právě zvolen tokový typ objektu. Nicméně jednu místnost si budeme definovat jako „trezorovou“, a proto bude v této místnosti odpovídat i zabezpečení, spolu s tím budou však pro účel projektu a názornost některé prvky předimenzované. Převedení zabezpečovacích prvků do grafické nadstavby díky integraci je totiž naprosto shodné i u větších typů instalací, jako jsou banky či firmy, případně muniční sklady hlídané armádou. Rozdíl je tedy pouze ve velikosti instalace a následném množství užitých prvků pro integraci do systému. Veškerá projektová a instalační práce je ovlivněna a vymezena v rámci platných zákonů, postupů a norem pro projektovou dokumentaci. V podsední řadě je nutné vybrat vhodný integrační grafický software, který bude uživatel/ochranka/operátor obsluhovat. Na českém trhu již existuje několik takových systému od různých firem. Například od firmy Trade Fides a.s. je to software Latis, Maxprogres s.r.o.nabízí svůj produkt pod názvem Accur8vision a firma Gamanet dodává na český trhsoftware C4. Všechny tyto produkty nabízejí kvalitní integrační nástroje, které se liší především v grafickémvzhledu. Pro náš modulový projekt si zvolíme software od slovenské firmy Gamanet a.s. její integrační produkt C4.

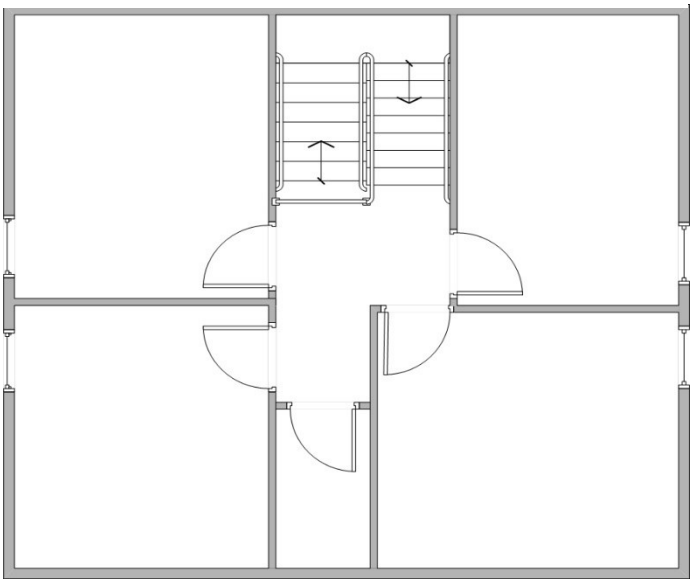
3.1 Zvolení umístění prvků v půdorysubudovy

Podle detailních dispozic modelového domu určíme vhodné možnosti ochrany a použití technologií pro náš projekt. Díky dokumentaci lze získat dostatečný přehled omožnosti rozmístění bezpečnostních technologiípo budově a v perimetru kolem budovy. V tomto projektu však nebudeme zohledňovat systémovou kabeláž, a proto se o ní nebudeme zmiňovat. Každý projekt má vyhotovenou projektovou dokumentaci pro všechny systémy s veškerou vedenou kabeláží a popisem všech prvků i s jejich adresací. My však budeme vycházet pouze z plánu budovy. K tomuto účelu se tedy velmi dobře hodí stavební dokumentace. Pro nás je vhodnější, pokud to lze si tuto dokumentaci zpracovat do přijatelné formy. Pro umisťování technologií budeme potřebovat zejména obrysy budovy a vnitřní uspořádání s rozměry, pokud prostory jsou větší rozlohy. Tato část není důležitá,

ale dá námperspektivnější pohled na věc. Tento krok lze udělat několika způsoby. Využitím příslušného softwaru pro překreslení plánů, čímž zpřehledníme situaci v objektu. Například použitím softwaru MS Vision, v kterém lze snadno překreslit potřebné záležitosti a zároveň umožňuje umisťovat komponenty do projektu. Další možností, jak provést úpravu jsou speciální programy jako je CAT, Solid Edge nebo NX které vyžadují už určitou dávku znalostí. Rozdíl mezi upravenou a neupravenu dokumentací lze porovnat z následujícíchobrázků níže (obr.11 a obr.12).

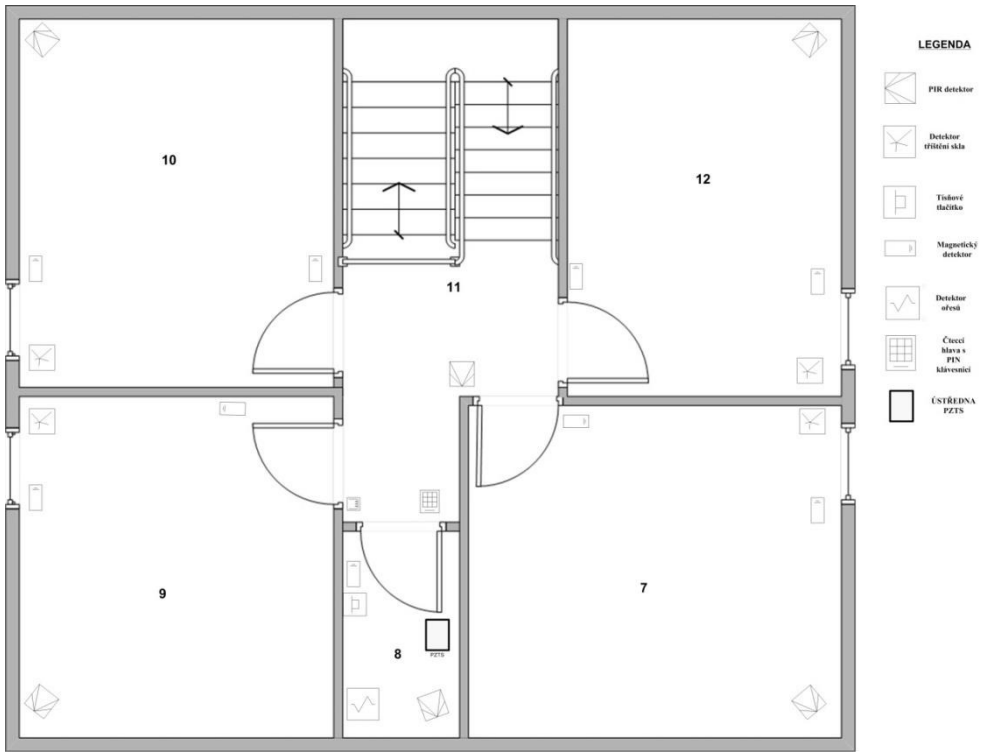


Obr. 12. Dokumentace modulového domu



Obr. 13. Upravená dokumentace pro umístění prvků

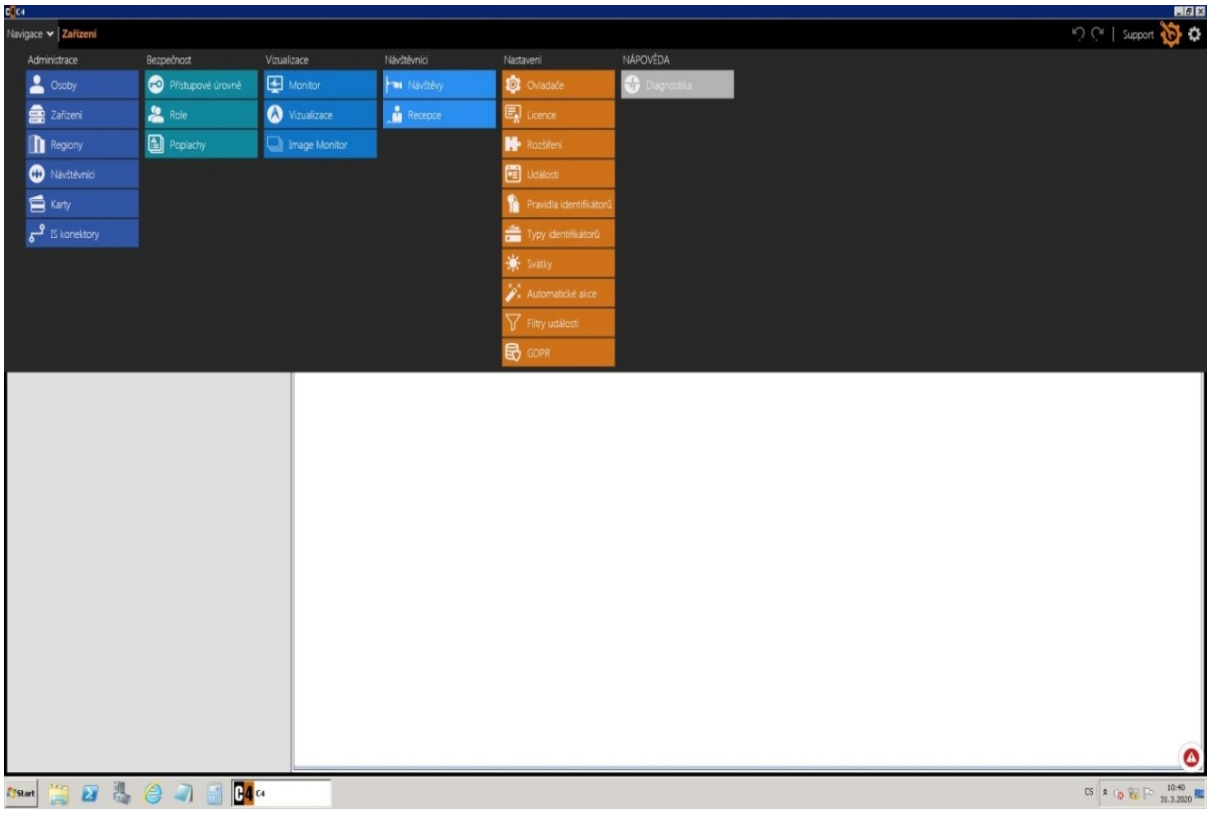
Rozdíl v přehlednosti mezi obrázky je zcela patrný. Takto vytvořený situační plán je již snadné doplnit o technologie, které potřebujme. V našem případě doplníme standardní prvky užívané v systémech EPS, PZTS, SKV a CCTV. Na následujícím obrázku je již zapracován plán rozmístění prvků PZTS spolu s řídící jednotkou systému a jednotlivé místnosti jsou opatřeny čísly k zajištění snadné orientace v objektu. Pro snadnou úpravu jsme využili opětovně MS Vision. Naprosto shodným způsobem se postupuje u všech ostatních systémů (CCTV, EPS, SKV), které jsou použity v projektu. Dále již nebudeme ukazovat úpravy ostatních systémů, protože identické s postupem u PZTS. Hotové podklady nám pak budou sloužit ke snadné orientaci v umisťování veškerých prvků právě v mapových podkladech grafického softwaru.



Obr. 14. Podklad PZTS pro modelový dům

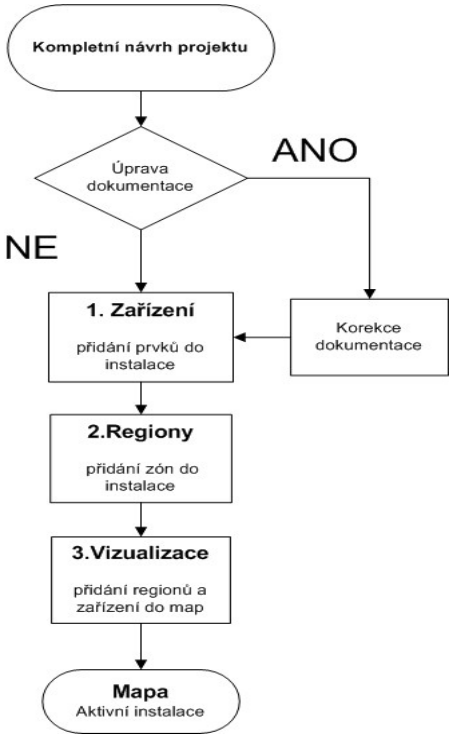
3.2 Integrační software v grafickém zobrazení

Každý integrační software má svá specifika pro zavádění bezpečnostních systémů pod jeho správu. My se zde budeme zaměřovat na systém, který jsme si zvolili, a tím je tedy integrační software C4. Jeho prostředí umožňuje snadnou a přehlednou administraci pro techniky i obsluhu. Má intuitivní rozložení prvků pro správu a přehlednost je umožněna díky použité čisté grafiky. Nebudeme se v této práci zabývat samotnými nastaveními přímo prvků v systémech, ale jen uvedením těchto prvků již funkčních v systémech do grafické nástavby. Základem softwaru jsou tedy korektně fungující ovladače pro všechny systémy (CCTV, SKV, EPS, PZTS), které jsou dodávaný firmou poskytující samotný software. Pokud to vyžaduje změna technologie je firmou vytvořen nový ovladač pro danou technologii a tím se zabezpečí opětovná bezproblémová komunikace. Součástí je též soubor licenci pro aktivaci všech použitých technologií. Pro převedení prvků do grafické nadstavby je u softwaru C4 potřeba provést několik nezbytných kroků, které si ukážeme v následujících částech. Na obrázku pod textem je ukázka základního přehledu všech nabízených funkčních možností C4.



Obr. 15. Základní administrační přehled množností C4

Z možností hlavní nábytky jsou pro násovšem nejdůležitější tři volby, kterým se budeme nadále věnovat. Jsou to nabídky: **Zařízení**, **Regiony**, **Vizualizace**. V těchto třech možnostech se děje vše, co je potřebné k nastavení a zprovoznění našeho projektu. Jak bylo zmíněno samozřejmostí je v nabídce **Ovladače** a **Licence** mít nainstalované ovladače a platné licence pro technologie použité v projektu. Na obrázku 16 je jednoduchý vývojový diagram ukazující přehledně postupné kroky pro realizaci naší instalace, respektive projektu.



Obr. 16 Rozfázování průběhu instalace

3.2.1 **Zařízení**

Prvním krokem v našem projektu, a i v každém dalším projektu, je propojení našeho software s prvky, které jsou součástí systému. Nemusí to byt přímo integrovaný systém zahrnující veškeré systémy, jako jsou PZTS, SKV, CCTV, EPS. Lze samozřejmě spravovat jen jeden z těchto systémů. Za pomoci adresace jednotlivých prvků se přiřazují k daným prvkům jejich specifické vlastnosti v systému a odpovídající grafické značky. V hlavní nabídce si zvolíme nabízenou možnost **Zařízení**, kde budeme tyto náležitosti spravovat a přepneme se tak do menu **Zařízení**, které je v základním nastavení. Z obrázku 17 je patrno, jakou má daná administrace strukturu. V levé části je předdefinovaná instalace, kterou jsme si na kartě **Obecné nastavení** pojmenovali

DUM.V tuto chvíli nejsou v zařízení žádné další prvky obsaženy a musí se tedy následně postupně přiřadit. K tomu nám slouží zmiňované adresy prvků použité v našem projektu. Lze též pozorovat na kartě **Obecné nastavení** číslo použitého portu, které je definováno samotnou instalací a pokud není nutné jej měnit, necháváme tuto hodnotu nezměněnou.

Obr. 17 Zařízení pro administraci

Dále máme k dispozici v tomto administrátorském prostředí další karty, jako **Události**, **Přístup**, **Odkazy**, **Přístupové úrovně**, **Typy identifikátorů**. Uvedené možnosti jsou v tuto chvíli pro naše účely nepotřebné. Jejich funkčnost přichází v platnost až v okamžiku, kdy je systém z cela nastaven a zprovozněn. Do té doby jsou dané možnosti neaktivní. Následující krok spočívá v rozhodnutí, který náš systémem zvolíme jako první k našemu zpracování a začneme ho začleňovat do instalace. Zda dáme přednost PZTS, CCTV, EPS, SKV. Přesná pravidla, která by určovala, který systém má být jako první zařazen do instalace nejsou nikterak definována. Proto si zvolíme jako první systém, který budeme do instalace zavádět PZTS. Bude ho následovat SKV, po tomto systému zavedeme CCTV, a nakonec přidáme EPS.

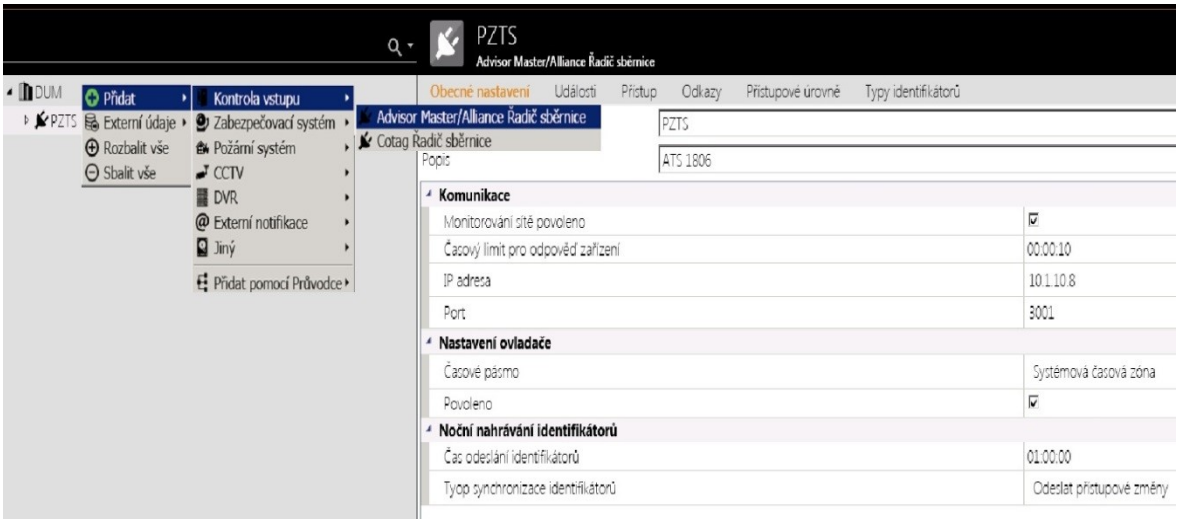
3.2.1.1 Zavedení PZTS systému

Pro jednoduší zavedení do systému nám poslouží naše upravená schémata, v kterých jsme si předem označili koncová čísla prvku. Dobrý pomocník může být i vytvořená tabulka s prvky a jejich adresami pro rychlejší orientaci a zadávání do systému. V našem případě byla zvolena první varianta. Na obrázku 18 můžeme vidět možnosti poskytované naším zvoleným softwarem C4. Postup zavádění různých systému do softwaru je v podstatě kopírování podle fyzického stavu instalovaného systému do softwarové podoby.

Označíme si naší instalaci nazvanou **DUM**, kterou jsme získali jednoduchým přejmenováním předchozího názvu **Instalace** a pomocí pravého tlačítka na myši vyvoláme menu. V menu máme k užití několik možností, jako je **Přidat**, **Externí údaje**, **Rozbalit vše** a **Sbalit vše**. Pro přidání prvků zvolíme pro nás jedinou možnou volbu **Přidat** a

v následném menu vybereme možnost **Zabezpečovací systém**. V tomto vyvolaném menu již zvolíme námi hledaný první prvek, a to jeATS 1806 (modul) univerzálního rozhraní zajišťující komunikaci mezi serverem a řídící jednotkou. Pro nás tedy volba **Advisor Master/ Alliance Řadič sběrnice,** jak je vidět na obrázku 18.Tato možnost pod sebou skrývá již instalované ovladače i potřební platné licence. Po potvrzení našeho výběru je do stromové struktury instalace přidán náš požadovaný prvek, jak je vidět na obrázku níže spolu s nastavenými hodnotami. Modulové rozhraní jsme si pojmenovali PZTS pro přehlednost a lepší orientaci v systémech. V pravé části obrazovky je k dispozici na kartě **Obecné nastavení** přehled těchto nastavitelných položek.

- Komunikace
- Nastavení Ovladače
- Noční nahrávání identifikátorů



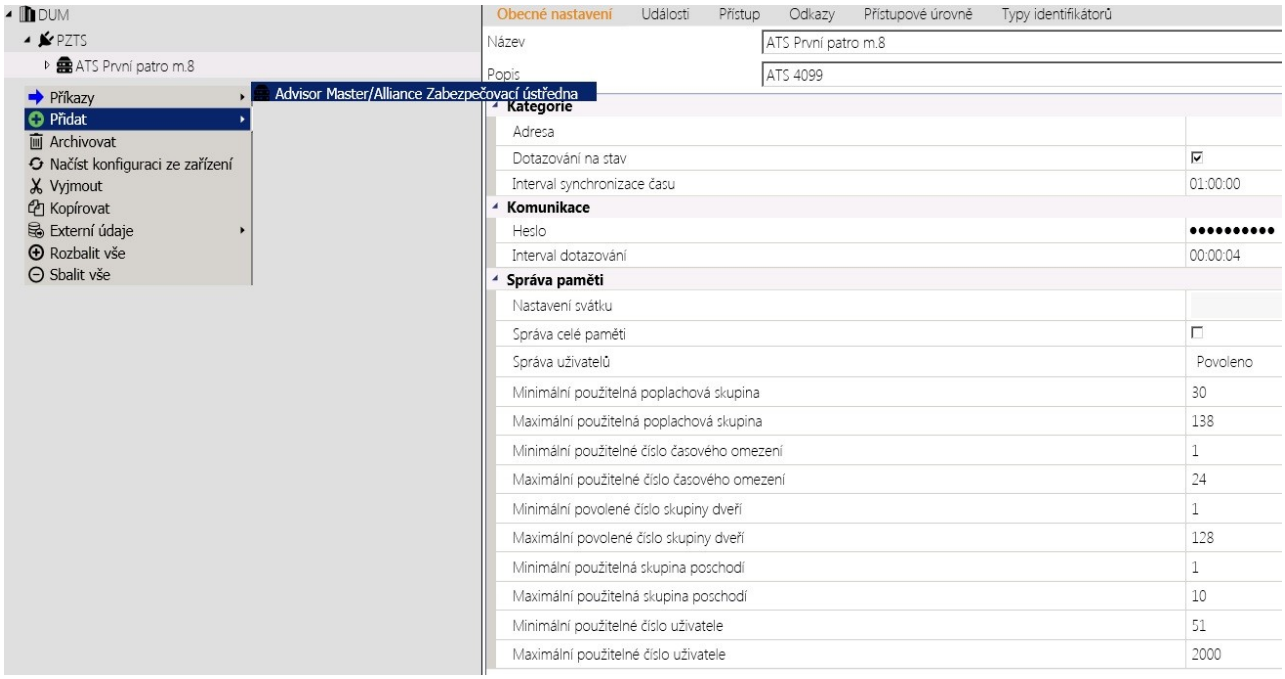
Obr. 18 Přiřazení univerzálního rozhraní pro PZTS a nastavení

V položce **Komunikace,** jak je patrno z obrázku jsme vyplnili IP adresu modulu a komunikační port. Veškerá komunikace systému běží prostřednictvím UDP protokolu po sériovém rozhraní RS 232. V komunikační části je možno též nastavit časový limit pro odpověď zařízení. Tuto hodnotu je dobře upravit dle specifikací a velikosti instalace. Základní hladina hodnoty této volby se pohybuje kolem 10 s. Pokud ale nastávají v instalaci problémy s komunikací a výpadky zařízení, je nutno navýšit limit pro odpověď kupříkladu na 30 s, aby mělo zařízení dostatek času ve velkých instalací možnost včas odpovědět. Jinak může docházet k tomu, že softwaredanou prodlevu v komunikaci vyhodnotit jako poruchu komunikace. Nutnost povolit ve stejné sekci monitorování sítě je

samozřejmostí, protože je tím zabezpečena kontrola komunikačního toku. V **Nastavení ovladače** máme pouze dvěmožnosti nastavení. První je **Časové pásmo**, které je pro nás nastaveno na standartní časovou zónu. Díky této možnosti máme možnost vybrat časová pásma dle geografické polohy instalace, ale v našem případě to nemá opodstatnění. Druhá možnost je nazvaná P**ovoleno**. Tímto nastavením se volí mezi zapnutím a vypnutímprvku tedy logicky je nutné tuto možnost povolit. Vypnutí této možnosti je dobré pouze vpřípadě, pokud je potřeba provádět softvérové úpravy v sytému a zamezit možného nechtěného znovu zapnutí komunikace se softwarem. Poslední kategorií nastavení v případěuniverzálního rozhraní je nastavení **Nočního nahrávání identifikátoru**. Tato část se opětovně dělí do dvou možností, jak je vidět z obrázku. Prvním nastavené rozhodujeme, kdy bude spuštěno nahrávání informací do našeho zařízení, která jsou napojená na dané rozhraní. V tuto definovanou dobu je dobré volit v časovém úseku, kdy je v objektu nejmenší pohyb osob. Poslední volbou je vybrat jaká forma bude v daném čase pro identifikátory zvolena. Možnosti jsou dvě. První je **Odeslání přístupových změn** a druhá **Vymazání paměti a odeslat všechny identifikátory**. My budeme volit první možnost. Protože tato volba v systému změní pouze změněné události, které proběhli od posledního nahrání identifikátoru. Tato volba je pro systém menší zátěží a je v porovnání s druhou možností mnohem časově úspornější. Pokud bychom zvolili druhou možnost budou během nahrávání kompletně smazány veškeré údaje ze zařízení a poté opětovně zpět nahrány. V tomto případěmluvíme dle velikosti instalace i o hodinách nahrávaní, kdy nelze zařízení použít z důvodu vymazaných dat. Zvláště v případě SKV systémů, kde mohou být i tisíce uživatelů.

Po nastavení veškerých parametrů pro naše rozhraní můžeme přistoupit k dalšímu kroku, a to přidání ústředny PZTS pod naší sběrnicí. V našem modelovém příkladu se bude jednat o ústřednu ATS4099. Na obrázku níže je vidět, že software již nabízí pouze jednu možnost, a to přidání ústředny. Zvolíme tedy jedinou volitelnou možnost, kterou máme a opětovně se dostaneme do stavu, kdy přidanou ústřednu budeme muset nastavovat. Nastavění ústředny se rozděluje do tří částí.

- Kategorie
- Komunikace
- Správa paměti



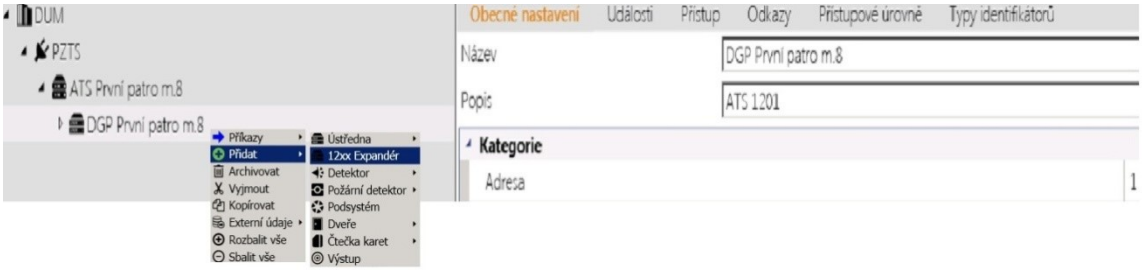
Obr. 19 Přidání PZTS řídící jednotky a nastavení

Kategorie je také rozčleněna do tří nastavitelných částí. První z nichje **Adresa**. Tu si nastavíme na hodnotu jedna, protože je to první zařízení připojené do našeho univerzálního rozhraní. **Dotazování na stav** je vždy povoleno. Jinak by nebyla umožněna komunikace ústředny se serverem. Poslední nastavení v této části je **Interval synchronizace času**. Je to velice důležitá funkce, kterou musíme nastavit na vhodnou hodnotu. Nejvhodnější volba je vždy brzo ráno. Ideálně kolem jedné hodiny ranní, jak je i nastaveno v našem případě. Ústředna se v této době spojí s časovým serverem a upraví si svoje vnitřní časové hodiny na ty v časovém serveru. Tímto je zaručeno, že všechny ústředny v celé instalaci mají jednotný a přesný čas. Pokud instalace nemá společné řízení času lze tuto funkcí přenechat přímo serveru, na kterém běží samotná aplikace našeho softwaru.

Komunikace je další část, kterou musíme nastavit. Je zde volba **Hesla** a **Interval dotazování**. Podobně jak je tomu u sběrnice, volíme hodnoty dle velikosti instalace. My si zvolíme dotazovaní 4 s. Volba hesla je pak pro přístup komunikace s rozhraním. **Správa paměti** je poslední možnost nastavení. První volba je pro nás nepodstatná. Jde o nastavení svátku, ale tato problematika je upravovaná samotným natavením možností průchodů v aplikace, a proto zde nevolíme žádnou možnost. Naproti tomu možnost **Správy celé paměti** má velice důležitou vlastnost. Pokud necháme tuto možnost zapnutou, budou veškeré náležitosti ústředny spravovány řadičem softwaru. My necháme možnost

nepovolenou, dostaneme se do následovného přehledu množství nastavení samotné ústředny, jak ukazuje předešlí obrázek. **Správa uživatelů** nastavíme vždy na možnost povoleno, jinak nebude přes ústřednu administrovat uživatele. **Minimální** a **Maximální použitelná poplachová skupina**. Tyto hodnotu necháváme na hodnoty předdefinované naším zvoleným softwarem. Případně můžeme změnit maximální hodnotu. Z důvodu použitého zařízení, v našem případě ATS, ovladače pro náš systém neberou potaz vnitřní uspořádáníústředny ATS. A jako nadstavbový systém C4 nemá kompletní vládu nad hardwarem v ATS. Pro administraci systému PZTS tvořenou ATS zařízeními je používán program Titan. Za pomocí tohoto softwaru se administruje celý hardware ATS systému. Ostatní možnosti ve **Správě paměti** jsou proto v C4 nechávány na předem definovaných hodnotách definovány ovladačem. Jako například Minimální použitelné číslo uživatele. V našem sytému je ukládání uživatelů pro použití ATS zabezpečení definován od čísla 51. Pokud je pozice uživatele menší tedy například 45 nebo 3, nebude systémem zaznamenávat údaje, protože tyto události nevidí a vypíše pouze obecnou událost například zóna zastřežena, ale neuvede, kterým uživatelemapod.

Po nastavení ústředny můžeme přistoupit k expandérům. V našem příkladně budeme do instalace přidávat dva expandéry ATS 1201. Na obrázku 20 je ukázka všech možností poskytnutých softwarem. My v této chvílí potřebujeme přidat do instalace pouze náš expandér. Proto volíme možnost 12xx Expandér a tím si požadovaný prvek přidáme do naší instalace. Poté již bude jako vždy potřeba nastavit parametry.

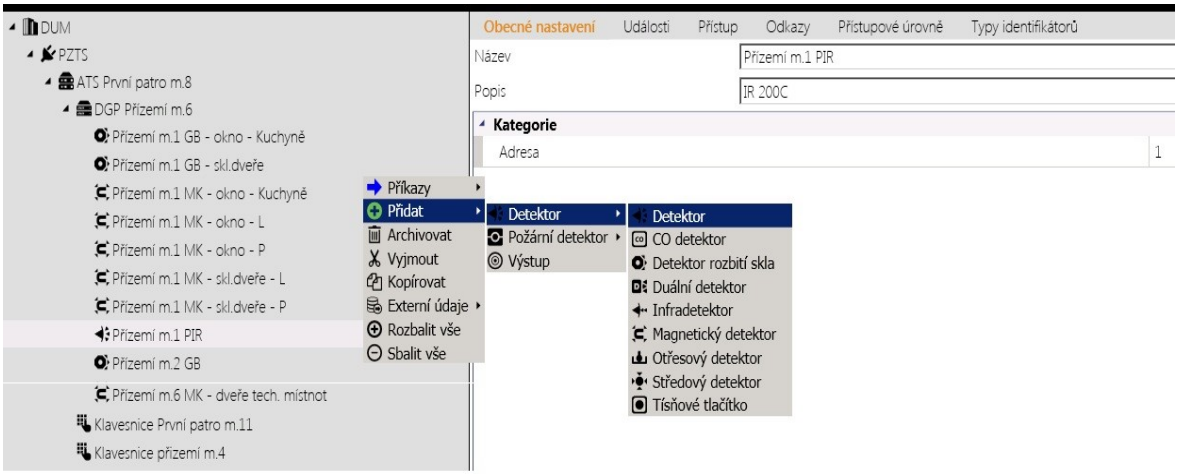


Obr. 20 Přidání DGP a nastavení

U těchto prvků je to ovšem již velice jednoduché. Po přidání daného prvku stačí pojmenovat prvek a v sekci **Kategorie** zadat adresu prvku v ústředně. Pro první prvek volíme adresu jedna a pro druhý, který přidáme totožným postupem adresu dvě případně hodnotu danou dle vlastností instalace. V další fázi přidáme do instalace ovládací prvky (klávesnice). Pomocí pravého tlačítka myši nad ikonou ústředny vyvoláme nábytku jak

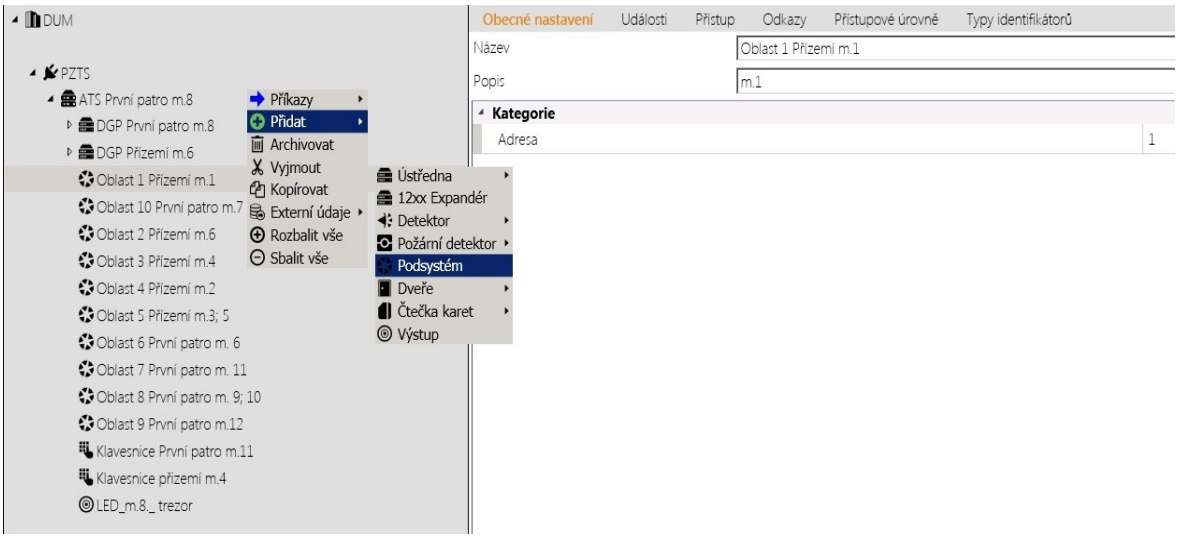
v předešlém případě. Přesunem se na možnost **Přidat** a poté směřujeme do možnosti **Čtečka karet**. V této nabídce již vybereme možnost **Klávesnice** a přidáme ji tímto krokem pod ústřednu, kde jí chceme mít. Tento krok budeme opakovat znovu a přidáme do naší instalace takto druhou klávesnici. Při každém přidání je nutné pojmenovat prvek a přiřadit mu adresu, jak bylo ukázáno u expandéru. Název prvků byl volen podle umístění v budově pro snadnou přehlednost. Pro naše účely je toto pojmenování dostačující, ale pro rozsáhlejší instalace je potřeba zvolit jiné preference pojmenování. Například pokud instalace obsahuje dvacet ústředen PZTS je vhodné si je v názvu očíslovat a toto číslo pak uvádět vždy jako první i uprvků pod danou ústřednou. Z toho je ihned patrno, k jaké ústředně dany prvek náleží, případně doplnit údaj o patro a označení části budovy.

Další krok po ukončení nastavení klávesnic je začít přiřazovat jednotlivé koncové prvky dle našeho schématu. My začneme přidávat do instalace vše, co máme umístěno v přízemí a umístíme tyto prvky do expandéru DGP Přízemí. Na obrátku 21 je vidět, jaké máme možnosti ve volbách prvků k přiřazení do instalace. Není opětovně definováno, kterým prvkem a kde začít, ale mi půjdeme dle místností od místnosti jedna až do místnosti šest. Začneme do expandéru přiřazovat prvky a prvním bude PIR detektor IR 200C. Z možností poskytnutou softwarem zvolíme tedy možnost **Detektor**, která zastupuje řadu prvků známých detektorů. V tomto menu vybereme opět možnost **Detektor** zastupující PIR detektory (a podobné zařízení). Prvek je tímto přidán pod zvolený expandér a musí se vhodně pojmenovat a přiřadit mu adresu dle naší dokumentace. Na obrázku 20 je vidět nastavení detektoru. V poli **Adresa** jsme uvedli číslo jedna, další detektory budou mít vždy o jednu hodnotu vyšší číslo. Opět zde platí, že dva prvky nesmějí mít stejná čísla.



Obr. 21 Přidání Detektorů a nastavení

Tímto způsobem budeme pokračovat pro všechny prvky v přízemí a následně budeme přidávat prvky do DGP První patro obdobným způsobem. Na obrázku 20 je pak možné shlédnut přidaná některá zařízení v instalaci v prvním patře a i klávesnice, které jsou připojeny přímo do ústředny. Pokud v instalaci vyžadujeme i signalizaci pomoci osvětlení, je možné do ní přidal led diodu signalizující stav zastřeženou či odstřižené oblasti. My takovou střeženou místnost máme v prvním patře s číslem 8 a je vidět na obr.14. Nastavení je shodné jako nastavení například PIR detektoru. V nabídce **Přidat** při vybrané ústředně zvolíme volbu **Výstup,** jak je vidět na obr.20, a tím přidáme světelnou signalizaci patrnou na obrázku.22 umístěnou na posledním místě v stromové struktuře. Nezapomeneme samozřejmě přidat prvku i adresu.



Obr. 22 Přiřazení podsystémů (oblastí) do instalace

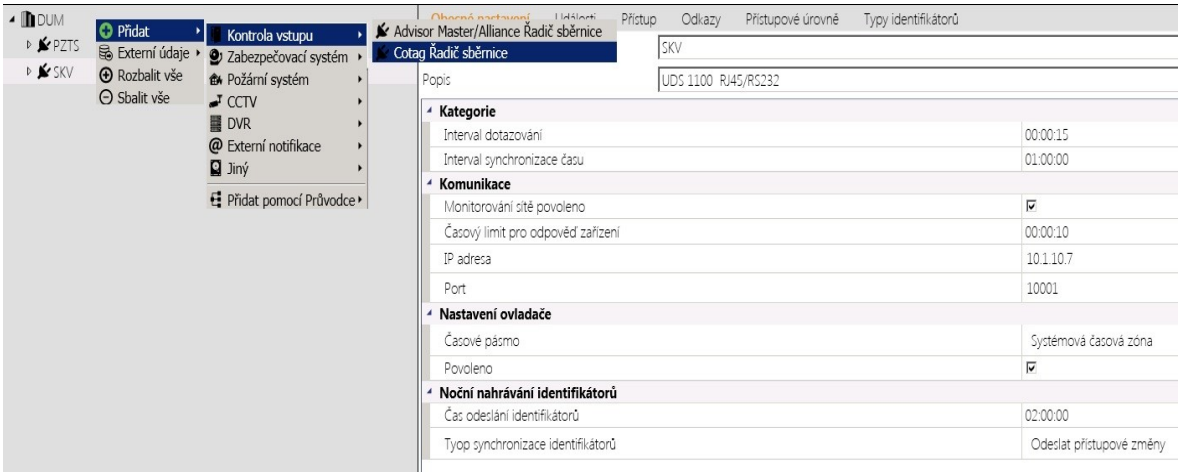
Po těchto krocích se dostáváme do finální fáze přidání PZSTS do naší instalace. Posledním krokem je umístit do systému zabezpečené zóny. Na obrázku pod textem je vidětmožnost softwaru pro přidání bezpečnostních zón, která je zde nazvaná **Podsystém**.

Potvrzením této možnosti je do instalace přidána zabezpečená zóna, kterou poté nastavíme. Opět tedy zadáme vhodný název pro oblast 1 a přiřadíme adresu jedna. Takto pokračujeme v přidávání dalších jednotlivých oblastí podle projektu. Pro náš modelový příklad přidáme do systému 10 zabezpečených oblastí a s částečná strukturu je vidět na obrázku 22, zároveň s nastavenou první oblasti. Nyní je celá PZTS uvnitř objektu přidána do instalace.

3.2.1.2 Zavedení SKV systému

Dalším systém, který budeme začleňovat do naší instalaceje systém SKV. V našem modelovém příkladu se bude jednat o jednotku SKV Cotag. K této naší jednotce budeme přistu-

povat prostřednictvím sběrnice UDS 1100. Aby instalace byla kompletní, bude jednotka osazena třemi hlavami PR 100 a jednou PP 500 spinovou klávesnicí. Samozřejmostí jsou i moduly pro připojení čtecích hlav a RF modul pro zajištění komunikace s tokeny zároveň se záložním zdrojem pro případ výpadku elektrické sítě.



Obr. 23 Přidání sběrnice pro SKV a nastavení

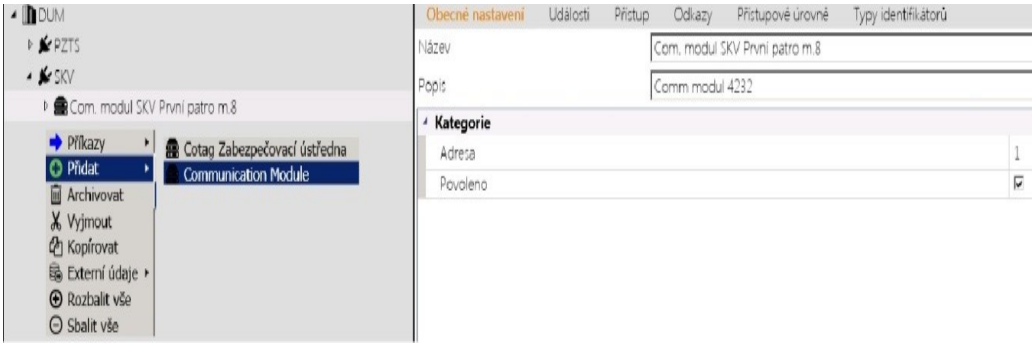
Opětovně si můžeme přidání zařízení rozfázovat. První bude přidání sběrnice pro komunikaci mezi počítačem (serverem)a ústřednou. Na obrázku 23 je vidět postup přidání této sběrnice do instalace. Poté, podobně jako u PZTS je nutné nastavit potřebné parametry pro sběrnici, jak je vidět také na obrázku 23. Přidání SKV sběrnice se provádí totožné jako přidání prvku u PZTS. Přes vyvolané menu vybereme možnost **Přidat**. Poté následuje volba z nové nábytky **Kontrola vstupu** a zde volíme možnost **Cotag Řadič sběrnice**, která nám přidá so instalace potřebnou sběrnici, kterou si pojmenujeme SKV.

U SKV systému máme tyto možnosti nastavení.

- Kategorie
- Komunikace
- Nastavení ovladače
- Noční nahrávání identifikátorů

V části **Kategorie** je možné natavitčasový horizont na dotazování zařízení, který stačí nastavit na 15 sekund. Další možností je **Interval synchronizace času**. Tuto možnost je dobré nastavit jako u PZTS, v čase, kdy je zařízení nejméně využívané. V druhé části **Komunikace** disponujeme možností nastavení komunikačního portu, který je již z výroby nastaven na 10001 pro UDS 1100. Tuto možnost není třeba měnit, pokud to naše instalace nevyžaduje a my tuto možnost tedy zachováme. Další v řadě je nastavení **IP adresy**

sběrnice, která je dána naším nastavením systému. Dále nastavujeme **Časový limit pro odpověď zařízení**. Zde je nutné opět zvážit velikost instalace a přizpůsobit tomu také tyto časy. Pro naší malou instalaci stačí 10 s i méně. Posledním nastavení v této kategorii je **Povolení monitorování sítě**, které je vždy aktivní jinak by komunikaci se zařízením nebyla možná. V třetí části nastavujeme možnosti **Nastavení ovladače.** Zde jsou dvě volby nastavení, a to **Časové pásmo** nastavené na systémovou časovou zónu a možnost **Povoleno** umožňující aktivaci případně deaktivaci, samotného zařízení. V poslední čtvrté části nastavujeme **Noční nahrávání identifikátoru**. Zde se nastavuje čas, když se budou informace odesílat do sběrnice a potažmo do všech ustředěn k sběrnici připojených. Doba se určuje vzhledem k rozsáhlosti objektu a důležité je zvolit dobu mimo provozování

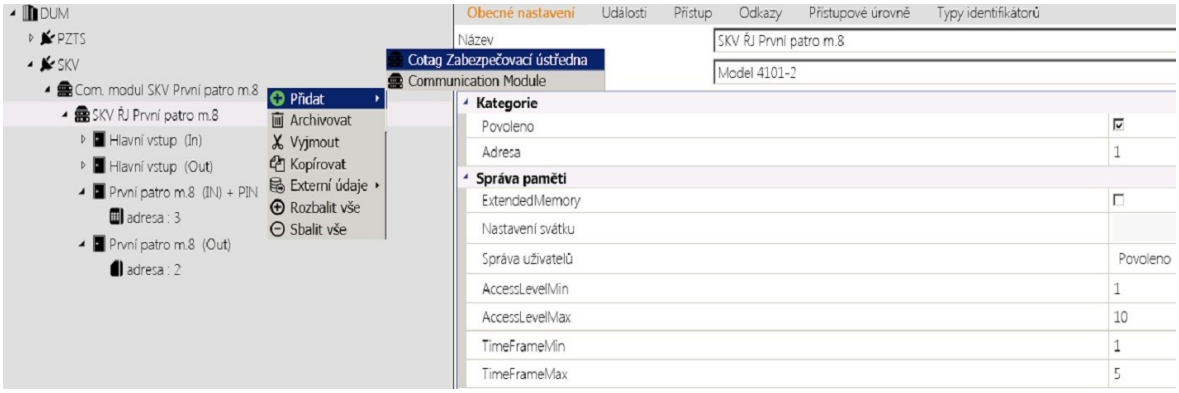


Obr. 24 Přidání komunikačního modulu

daného zařízení. Poslední možností se volí typ synchronizace identifikátorů. Zde volíme možnost **Odeslat přístupové změny**. Druhá možnost by byla **Vymazat paměť a odeslat přístupové změny**. Tuto možnost můžeme volit pouze v malých instalacích. Doba vymazání a opětovného nahrání osob je velice zdlouhavá a podobu nahrávanínefungují zařízení z důvodu prázdné paměti, protože nejsou v nich obsažené informace o uživatelích. Tedy volba času spadá také na dobu, kdy je v objektu minimum osob. Problematika je stejná jako u PZTS systému. Po ukončení této činnosti je čas na přidání dalšího prvku do instalace. A tím je komunikačního modulu, který bude zajišťovat komunikaci se sběrnicí a s ústřednou. V našem případě využijeme starší typ ustředěn Cotag MK2. Ta nedisponuje oproti MK3 připojením přes ethernet na základní desce a potřebuje proto ke komunikaci právě náš komunikační modul. Opětovně pomocí pravého tlačítka myši vyvoláme menu pro přidání komponent a volíme z nabídky**Komunikační modul**, který posléze nastavíme. Na obrázku 24 je ukázka nastavení tohoto modulu.

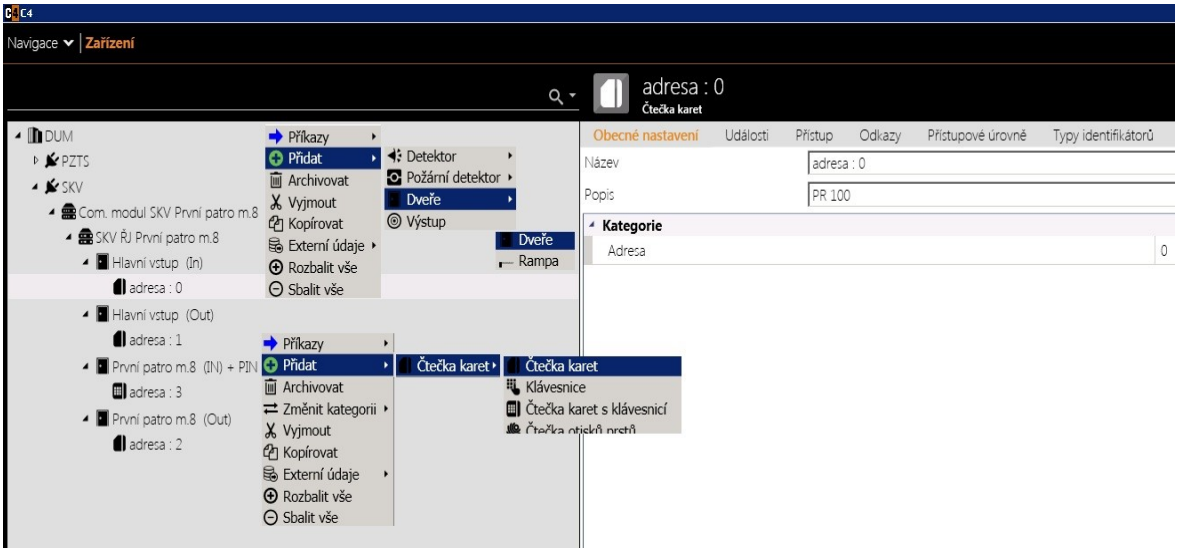
U tohoto prvku nastavujeme pouze adresu, kterou dáme na hodnotu jedna, protože je první v řade a povolíme zařízení. Tím je komunikační modul přiřazen a nastaven v naší instala-

cia lze tedy pokračovat v přiřazení samotné ústředny SKV pod tento modul. Jedná se, jak bylo již zmíněno o starší model ústředny 4101- 2 bez ethernetového připojení. Na obrázku 25 je vidět nastavení SKV ústředny spolu s celou strukturou SKV.



Obr. 25 Přidání řídící jednotky SKV a nastavení

Nastavení je rozděleno do dvou složek **Kategorie** a **Správa paměti**. V části kategorie zvolíme adresu a zadáme jí na hodnotu jedna, protože jde o první ústřednu v řadě připojenou na modul. V druhé části povolíme možnost použití zařízení. Ve správě paměti nastavíme vhodnou hodnotu u Timeframe (časové rámec). Jde o námi specifikované časové rámce, které budou přiděleny osobám využívající dané přidělené vstupy. Pro naší malou modelovu situaci stačí dát maximální hodnotu na pět. U nastavení AccessLevel (přístupové úrovně) jde o stejný případ a nastavíme na hodnotu 10, ale můžeme dát i nižší číslo. Po nastavení daných parametru přikročíme k přidání čtecích hlav do instalace. Jako první se přidávají dveře a k nim posléze se přidá čtecí hlava, a to klasická nebo s pin klávesnicí podle daného požadavku. Na obrázku 26 je k vidění možnosti volby pro přidání dveří a čteček. Podle požadavků vybereme potřebný prvek a poté ho nastavíme. V tomto případě se nastavuje pouze adresa pozice u čtecích hlav, do které je v ústředně připojena. My budeme mít čtyři čtecí hlavy a jedna z nich bude s pinovou klávesnicí. Samozřejmostí je, že vyvolané nabídky vždy odpovídají vybraným prvkům, pod které budeme přidávat následující zařízení. Na obrázku Obr.26 jsou k vidění dvě možnosti ve výběru. Horní nabídka patří pro přidávání dveří, zatímco máme označenou ústřednu. Spodní nabídka pro přidání čtecích hlav, zatímco máme vybrané dveře. Tímto krokem jsme dokončili přidání SKV do naší instalace a můžeme pokračovat v přidání EPS.



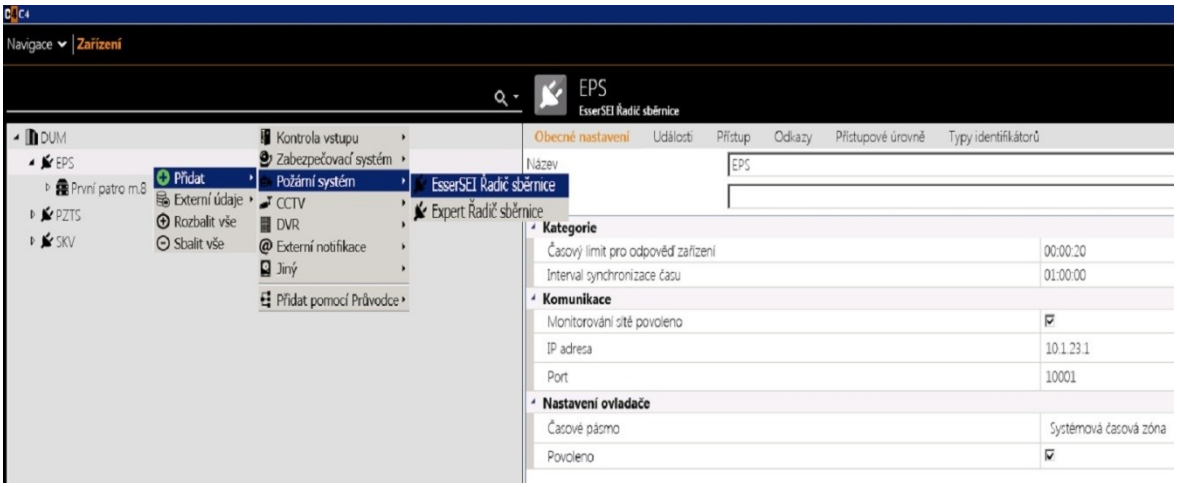
Obr. 26 Přidání dveří a čtecích hlav do instalace

3.2.1.3 Zavedení EPS systému

Přidání EPS systému do instalace probíhá dle stejných pravidel a postupů jako u předchozích systémů. Přes vyvolávací menu na instalaci vyvolámenabídku, kde zvolíme v možnostech**Požární systém.** V této nabídce vybereme možnost **EsserSEI Řadič sběrnice,** zajišťující komunikaci s požární ústřednou a naším softwarem na kterou se bude připojovat samotná EPS ústředna. Nastavení sběrnice je podobné jako u ostatních komunikačních modulů. V možnostech nastavení máme tyto volby.

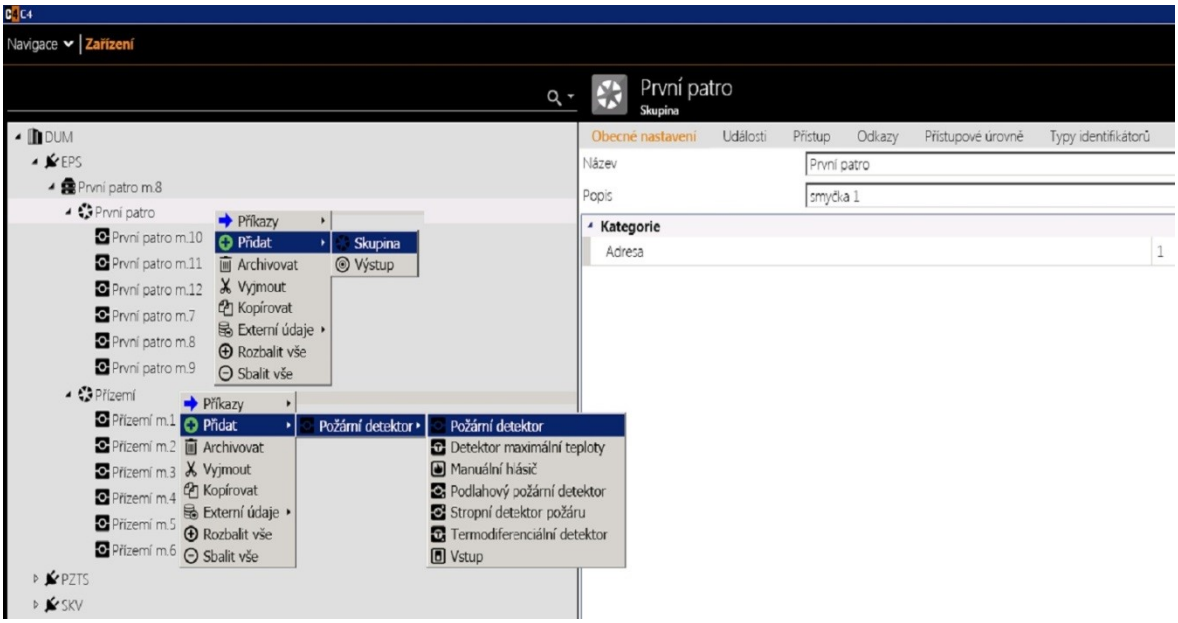
- Kategorie
- Komunikace
- Nastavení ovladače

Kategorie nastavuje dobu synchronizace času a časového limitu pro odezvu zařízení, kde vybereme hodnotu odezvy na 20 s. Doba synchronizace je daná na ranní hodinu z důvodu menšího provozu. U **Komunikace** nastavujeme IP adresu a komunikační port s povolenou možností monitorování sítě. Adresa je nastavená dle našich specifikací a port zůstává nastaven na základní hodnotu, pokud není potřeba ji měnit. **Nastavení ovladače**definuje možnost časového pásma spolu s možností zařízení aktivovat nebo deaktivovat. U nastavení časového pásma volíme systémovou časovou zónu jako u předešlých systémů. Nastavení je možné zhlédnou na obr. 27 i s ukázkou možnosti přidání sběrnice.



Obr. 27 Přidání EPS systému do instalace a nastavení

Ústřednu EPS přiřadíme do instalace pod sběrnici velice jednoduše. Přes menu zvolíme možnost **Přidat** a pokračujeme ve výběru na možnost **Esser SEI Požární ústředna**. Tento kroknaši ústřednu zařadí, kam potřebujeme. Veškeré výběry, které nám software nabízí, jsou vždy spjaté snainstalovanými ovladači. Bez nich by nebylo v možnostech výběru co volit. EPS ústředny nemají v rámci nastavování příliš možností oproti PZTS ústřednám. Zde nastavujeme v části **Kategorie** pouze adresu. Tato hodnota souvisí s pozicí v instalaci. Tedy my máme pozici první a z toho plyne nastavení adresy na hodnotu jedna. Následovat bude přidání požárních hlásičů. V první řadě si však musíme vytvořit skupiny (smyčky) do kterých se budou požární hlásiče přidávat. My budeme mít dvě skupiny, a to První patro a Přízemí. U skupin i hlásičů nastavujeme pouze jednu hodnotu v části **Kategorie,** a to u adresu. V našem případě bude nastaveno u smyčky První patro hodnota jedna a u Přízemí bude hodnota dvě. Poté se do těchto skupin přidají samotné požární hlásiče s adresou dle naší instalace. Pro nás bude adresace prvků dána od hodnoty 10 do hodnoty 21, protože máme 12 místností a každou vybavíme požárním hlásičem. Na obrázku 28 je k vidění možnost přidání skupiny a požárního hlásiče.



Obr. 28 Přidání smyček a požárních hlásičů do instalace

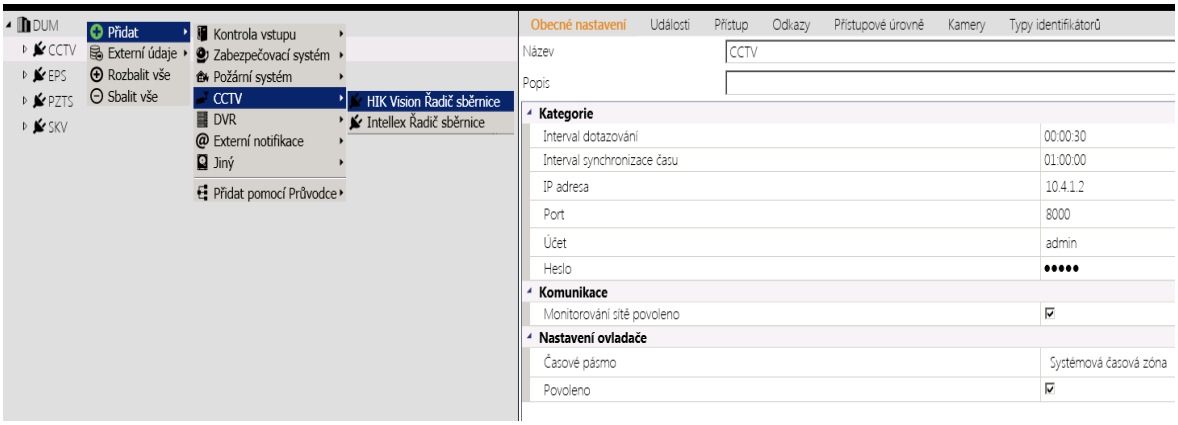
Z ukázky voleb na obrázku je u požárních hlásičů přehledný rozpis všech hlásičů, jenž lze softwarem přidat. My vybíráme možnost **Požární detektor,** ač název není adekvátní vzhledem k požární terminologii. Také máme možnost v obrázku vidět celou sestavu EPS systému a jeho rozložení do našich místností v budově. Tímto je požární systém zaveden do instalace a my pokračujeme se zavedením posledního systému, a to CCTV.

3.2.1.4 Zavedení CCTV systému

Posledním krokem pro náš projekt je zavedení CCTV systému do instalace. U systému CCTV postupujme podle zažitých procedur z dřívějších systémů. Prvním krokem je zavedení komunikačního modulu či řadiče (pro nás samotný DWR) a poté jsou k tomuto prvku připojovány ostatní zařízení. Jak bylo nastíněno prvkem, který budeme připojovat je záznamové zařízení Hikvision DS-7216 HUHI – K2. Pomocí vyvolaného menu přes příkaz **Přidat** vybereme možnost **CCTV** a vněm volbu **HIK Vision Řadič sběrnice**. Tímto přidáme naše zařízení do instalace a následně nastavíme potřebné hodnoty. Na obrázku 29 je vidět přidání a nastavení záznamového zařízení.

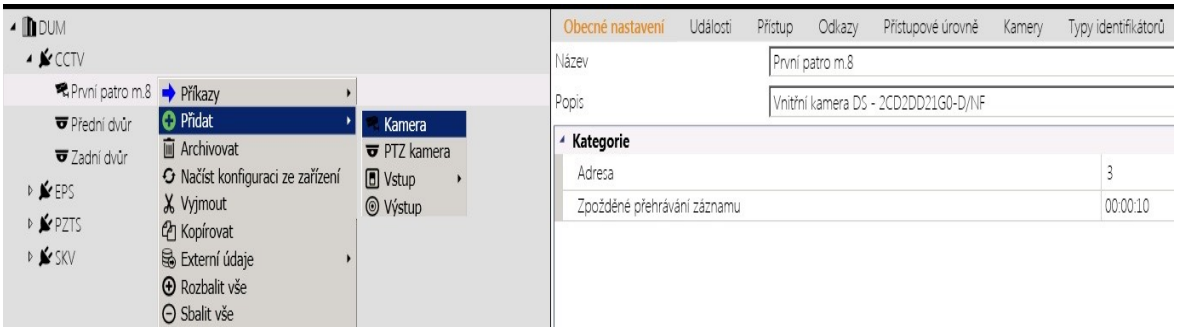
Náš software nám dává možnost u záznamového zařízení nastavit tři složky.

- Kategorie
- Komunikace
- Nastavení ovladače



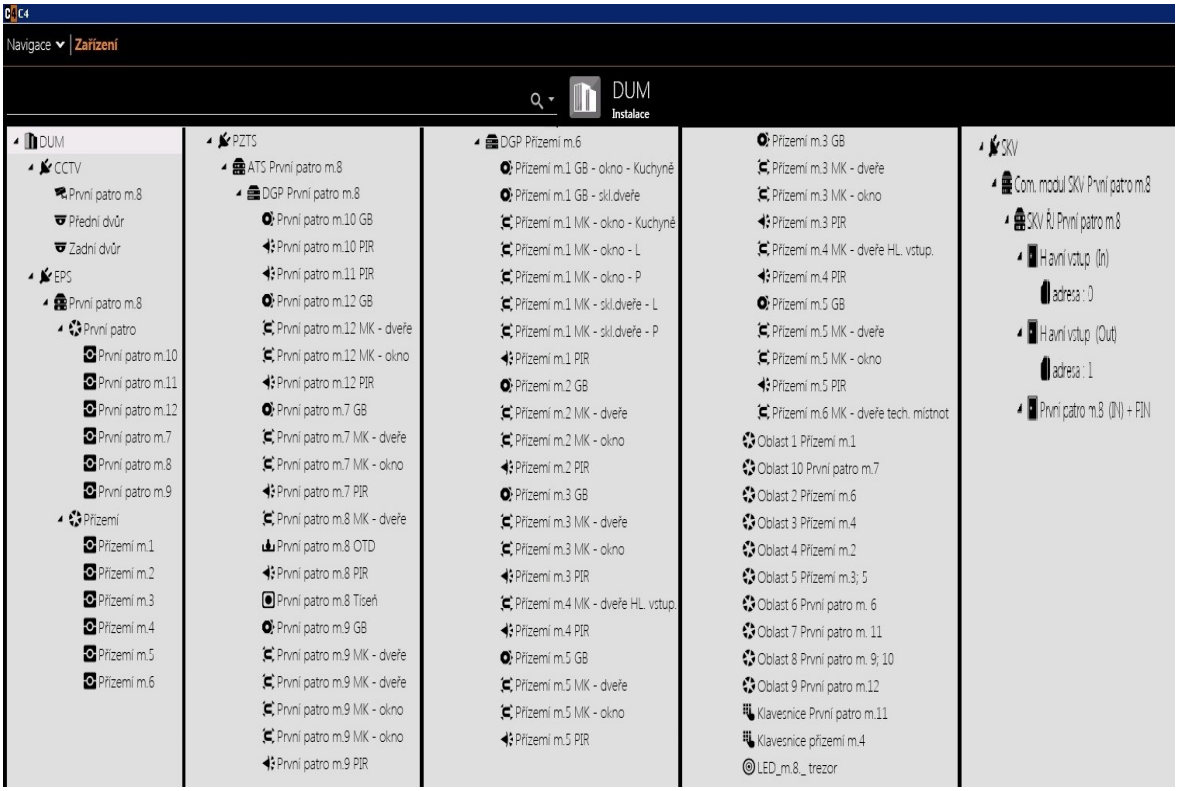
Obr. 29 Přidání záznamového zařízení do instalace

V části **Kategorie** nastavujeme dobu dotazování a také dobu synchronizace času. Nechybí ani nastavení IP adresy záznamového zařízení s číslem portu. V posledním úseku je název účtu s heslem pro správu daného zařízení. V části **Komunikace** a **Nastavení ovladače** se nastavují stejné parametry jako u předchozích systémů. Dále bude naše instalace obsahovat tři kamery. Dvě kamery budou otočné venkovní a jedna vnitřní umístěna v místnosti č. 8 v prvním patře. U kamer se nastavuje pouze v části **Kategorie** adresa kamery a čas zpožděni záznamu, který si nastavíme na 10 s. Přes vyvolávací menu vybereme možnost **Přidat**a v následném okně již vybereme potřebnou kameru, kterou nám nabízí software**.** Pro naše účely tedy vybereme volby jak **PTZ kamera,** jež zatupuje otočnou kameru tak i klasickou kameru zastoupenou volbou **Kamera**. Tímto postupem přidáme všechny tři kamery do instalace a přiřadíme adresy tedy od jedničky do tří s časovým zpožděním záznamu nataveným na 10 s. Na obrázku 30 je vidět přidání i nastavení kamery.



Obr. 30 Přidání kamery do instalace a nastavení

Tímto posledním krokem jsme ukončili první fázi našeho projektu. Dostali jsme do instalace všechna naše zařízení a natavili potřebné hodnoty. V další fázi budeme vytvářet regióny do kterých naše prvky budeme umisťovat v závislosti na našem projektu. Celá naše struktura instalace složená ze všech prvků je vidět na upraveném obrázku 31, aby byl obsažen veškerý obsah naší instalace. Vše je řazeno z hora dolu a z leva doprava.



Obr. 31 Přehledné zobrazení všech námi přidaných prvků do instalace

3.2.2 **Regiony**

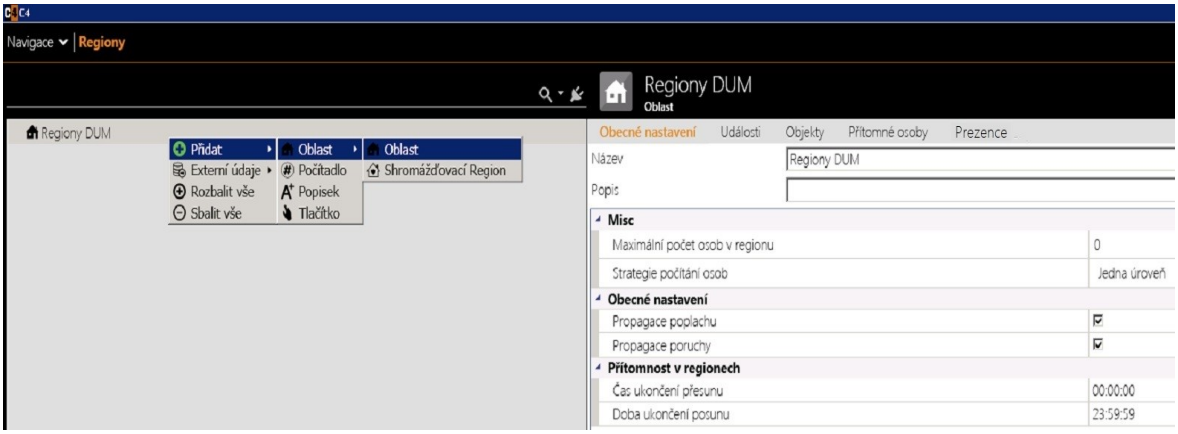
Druhá fáze nutná pro vytvoření našeho grafického podkladu pro projekt jsou regiony. V našem použitém softwaru C4 jsou hlavním bodem určující možné varianty uskupení prvků dle našich požadavků. Zde určíme, do jaké oblasti budou jednotlivé prvky zařazeny a které prvky budou pod správou těchto oblastí.

V první řadě se přepneme za pomocí volby Navigace z oblasti **Zařízení** do oblasti **Regiony**, která je též součástí administrace. Na začátku si naší instalaci přejmenujeme na Regiony DUM. Po přejmenování nastane správná doba na přidání první oblasti v regionu. Pro naše účely bude první oblastí PZTS. Předtím však musíme nastavit samotný Region DUM.

V možnosti nastavení máma tři základní kategorie nastavení.

- Misc
- Obecné nastavení
- Přítomnost v regionech

Tyto možnosti jsou totožné i u nastavováníoblastí a podoblastí, proto se nastavují u všech totožné parametry. Na obrázku 32 je k vidění nastavení oblastí za pomoci vyvolávacího menu (pravé tlačítko u myši).

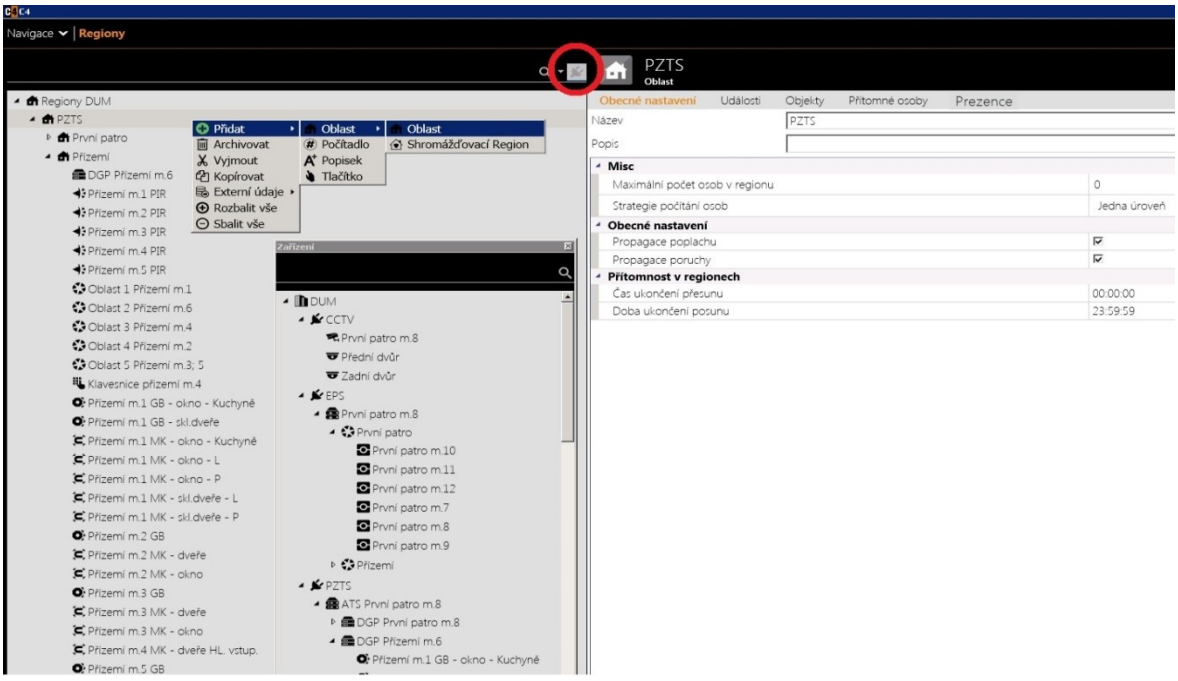


Obr. 32 Přidání nastavení regionu (oblastí)

U přidaných samotných prvkůdo oblasti zůstává možnost nastavení pouze **Obecné nastavení**, u které se povoluje pouze propagace poplachu spolu s propagací poruch. Obě možnosti musejí být povoleny, jinak by se neprojevovali v grafické vizualizaci změny u prvků. Tato změnadeterminuje vizuální kontrolu a stav zařízení u těchto prvků. Ostatní volby jako Události, Objekty, Přítomné osoby, Prezence nejsou použitelné pouze u živé instalace. Nicméně již z názvu lze usoudit účel jednotlivých složek. Možnost **Misc** obsahuje dvě nastavitelné položky, a to **Maximální počet osob v regionu** a **Strategie počítání osob**. Maximální počet osob v regionu nastavíme na hodnotu nula. Znamená to, že nechceme zastřešovat maximální počet možných osob v regionu. V našem případě je tímto nastaveno maximální počet osob, který může vstoupit. Pokud je z nějakého důvodu nutné počet osob v oblasti regulovat a umožnit vstup určitému počtu osob nastavíme hodnotu na danou hodnotu. Po dosažení této hodnoty nebude systém nadále další osoby do této oblasti pouštět. **Strategie počítání osob** má dvě volby. My použijeme první, kterou je **Jedna úroveň**. Tímto budeme definovat počítání v regionu na jednotlivé oblasti. Druhá možnost by pak byla **Celý strom,** což je na druhou stranu počítání osob ve všech regionech

a oblastech dohromady. Poslední možné nastavení je **Přítomnost v regionech**. Tato možnost nastavuje časový úsek, v němž bude daný region, případně oblast zaznamenávat osoby. My si zvolíme nepřetržité sledování a zadáme časový interval 24 hodin. Na obrázku víše je ukázka tohoto nastavení. Tímto posledním krokem jsme nastavili hlavní region. Další oblasti se nastavují totožně, jak již bylo dříve zmíněno.

Jak jsme si již zvolili, prvním krokem bude nastavení oblastí pro PZTS. Za pomoci rozbalovacího menu vybere pod Regionem DUM oblast anazveme si jí PTZS. Tu nastavíme shodně s hlavním regionem a podle našeho plánu přidáme do této oblasti další dvě podoblasti. Jedna bude mít na starosti přízemí a druhá první patro. Následuje přidání veškerých prvků, které tyto oblasti budou obsahovat. Tento úkon se provádí pomocí ikony,  která zapíná či vypíná volbu okna **Zařízení**. Na obrázku 33 je umístěna v červeném kruhu Okno **Zařízení** obsahuje celou strukturu instalacejiž námi vytvořenou v první fázi. V tomto okně lze pomocí funkce. Drag and Drop“(táhni a pusť) přemístit potřebné prvky do jednotlivé oblasti. Stačí tedy v tento moment vybrat ze zařízení PZTS prvky a rozmístit je do patřičných oblastí dle našeho návrhu. Na obrázku 33 je vidět také okno se zařízením a částečně přidanými prvky v oblasti PZTS **Přízemí**. Tímto snadným a rychlím postupem přidávání prvků do jednotlivých oblastí, vytvoříme veškerou strukturu požadovaných oblastí v naší instalaci pro systémy EPS, SKV, CCTV a PZTS.Po ukončení tohoto procesu již můžeme přejít do poslední třetí fáze kompletace grafického zobrazení **Vizualizace**.



Obr. 33 Zobrazení Regionů společné se Zařízením

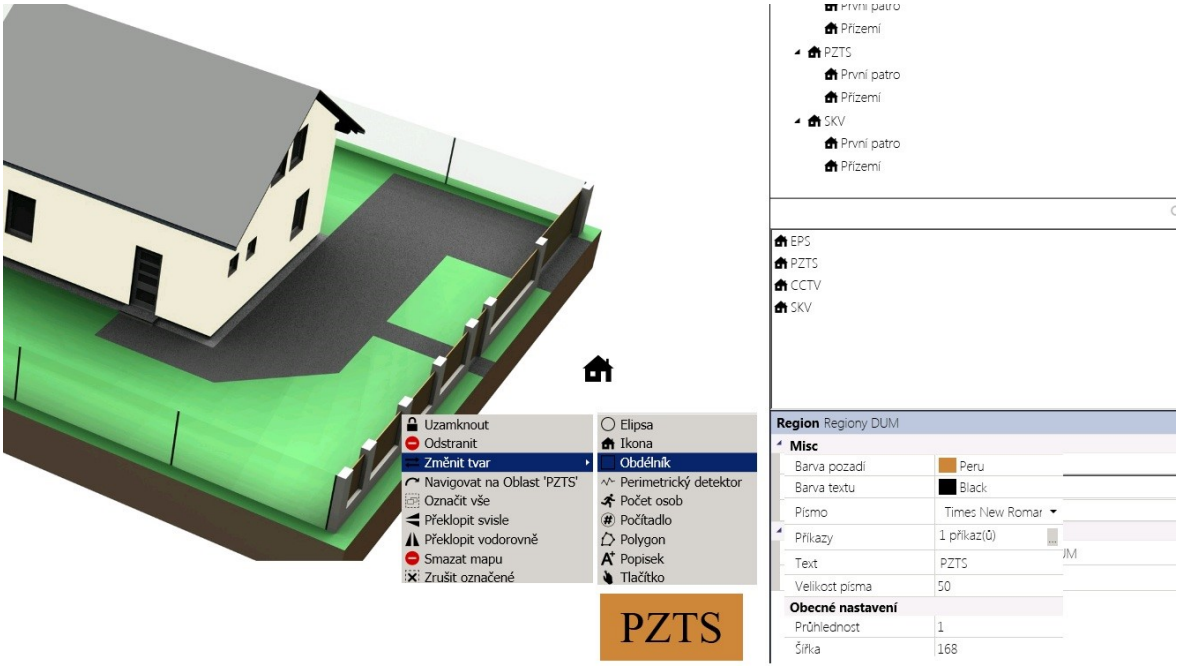
3.2.3 **Vizualizace**

Poslední, třetí fáze je kombinace předchozích dvou kroků s mapovým podkladem do jednoho funkčního celku. Pro tuto možnost se musíme za pomoci navigace přepnout do prostředízvané **Vizualizace**, kde jsou umožněný grafické úpravy. Na obrázku 34 máme k vidění základní vizuální zobrazení tohoto prostředí. Je zde již i vidět zobrazení našeho projektového domu spolu s rychlými odkazy na patřičné systémy. Na pravé straně v horním okně jsou k dispozici přehledně viditelné, námi již vytvořené oblasti či regiony obsahující po jejich výběru a načtení i přehled obsažených prvků přiřazené pro danou oblast, které jsou k vidění přehledně v prostředním okně. Dolní okno obsahuje možnosti změny barev a souřadnicové umístění prvků v mapovém podkladuči k další úpravy umožňující vizuální změny prvků. S tímto oknem se pracuje intuitivně a po kratším užívání lze sním již snadno pracovat. V horním okně, jak je vidět z obrázku máme k dispozici tří úrovně zobrazení instalace. **Regiony** zobrazují strukturu, kterou jsme si vytvořili v druhé fázi. **Zařízení** zobrazí instalaci vytvořenou v první fázi projektu. Možnost **Jiné** zobrazuje prvky, jako jsou počítadla a popisky, ale pro náš projekt nepotřebné. Naším prvním krokem bude umístit námi vytvořené mapové podklady do hlavního okna. Zobrazení manu je vidět na obrázku 34. Přes možnost pravého tlačítka u myši na hlavním okně vyvoláme menu, kde vybereme možnost **Přidat obrázek mapy**. Jsou zde dvě další možnosti, pro náš účel opět však nepotřebné. Jedná se o možnost **Označit vše** a **Přidat mapu AutoCAD**. Obě možnosti vystihují přesnývýznam úkonu, který provádějí. Po zvolení funkce **Přidat obrázek mapy** dohledáme na HDD místo uložení naší mapy a potvrdíme. V tomto okamžiku se zobrazí mapový podklad pro náš vybraný region či oblast. Mapa se poté načte a zobrazí jako na obrázku níže.

Obr. 34 Zobrazení vizualizačního prostředí

Z prostředního okna za pomocí funkce Drag and Drop (táhni a pusť) rozmístíme do správných pozic naše prvky. Tedy zkráceně vždy si vybereme v horním okně dany region, k němu vybereme potřebnou mapu a do této mapy z prostředního okna přidáme zařízení, jenž dany region obsahuje. Pokud máme v plánu vytvořit například odkazový prvek pro rychlou přepínající volbu mezi mapami jako u obrázku 34, jde o totožný proces. Za pomoci funkce Drag and Drop vybereme, na kterou část chceme odkázat. V našem případě budeme odkazovat z hlavní mapy (hlavní region) na PZTS oblast budovy. Tuto funkci v mapě přidáme tak, že si označíme Region DUM v horním okně. V prostředním okně se zobrazí obsah tohoto regionu. V něm vybereme region (oblast) PZTS a přetáhneme jí na mapu, kde se zobrazí ikona daného regionu. Na obr. 35 je vidět, jakou má po přetažení oblast ikonu. Po umístění na mapu přes pravé tlačítko vyvoláme menu a vybereme v něm možnost změnit tvar, tedy pro náš účel volíme **Obdélník**. Z obrázku lze vidět i přehled možných voleb, které nám software nabízí a vybrat si potřebnou volbu. Ve spodním okně si zvolíme vhodnou barvu případně další grafické úpravy, které budou odpovídat naší představě vizualizace. Předešlí krok budeme znovu opakovat a místo tvaru obdélníku zvolíme tentokrát tvar **Popisek**. Opětovně pomocí dolního okna upravíme popisek a jeho vlastnosti podle naší představy. Náš popisek přesuneme do obdélníku, a tím získáme grafický efekt připomínající tlačítko. Pro lepší efekt upravíme rozmístění obou prvků za pomoci vycentrování obrazců. Tímto postupem pokračujeme i u ostatních systémy. Pokud jsou tyto kroky příliš zdlouhavé, lze využít i jednoduší metodu. V menu změny tvaru vybereme možnost **Tlačítko.** Tím je odkaz přidán. Stačí v dolním okně změnit barvu

pozadí, přidat a pozměnit text (tvar, velikost, barvu). Výsledek není tak graficky výrazný, ale funkce je stejná. Výsledek obou možností je vidět na předchozím obrázku 34, kde horní přehled systému je tvořen první metodou. Pomocí kombinací těchto kroků lze docílit potřebné grafické úpravy pro obsluhu k zajištění rychlejší orientace a pohybu po objektu. Dalšími úpravami a manipulaci s tvarem objektů lze dosáhnout působivých grafických scenérií, které přehledněodrážejí skutečný stav objektu a jeho zabezpečení.



Obr. 35 Ukázka přidání a modulace prvků

Touto cestou se postupně připraví celá naše instalace ve vizualizačním prostředí dle našich představ a daných specifikací.

3.2.4 Mapa

Funkční zobrazení prvků v mapovém podkladu C4, která již slouží pro účely dohledu je kombinací tří postupných akcí. Zavedení všech prvků v celém systému do prostředí softwaru prostřednictvím Zařízení přes definici Regionů a jejich umístěním v rámci Vizualizace vytváří funkční dynamickou mapu. Přes možnost **Navigace** si zvolíme **Monitor**. Takto se dostaneme do naší vytvořené funkční mapy neboli monitoringu hlídané oblasti. V tomto prostředí obsluha kontroluje střežený objekt. Samozřejmostí je i vzdálený přístup, ke všem prvkům v instalaci. Tento přístup umožňuje ovládání jednotlivých zařízení celého systému, jako resetování detektorů, zastřežení zón, vynechání prvků apod. V následujících obrazcích je přehled systému PZTS jak je vidět z pozice obsluhy. Na ukázkovém obrázku 36 monitoringu je ke spatření celý náš hlídaný objekt. V dolním okně jsou pro obsluhu k dispozici aktuální údaje ve volbě **Události**. Veškerá činnost, která se

Obr. 36 Zobrazení projektu pro operátory

děje na daném objektu je zde zobrazena a obsluha má k dispozici veškeré aktuální informace. Druhá možnost v tomto okně je **Historie**. Zde si obsluha dohledává vznik události v určitém časovém období, například vznik poplachů apod. Levé okno slouží k rychlému přehledu stromu regionů, a pokud se vybere možnost **Vynechaná zařízení** má obsluha ihned přehled o všech zařízeních na objektu, které jsou deaktivovaná. Tato možnost je zvlášť účelná pro velké instalace, kde jsou stovky a ž tisíce zařízení. Pro přesun

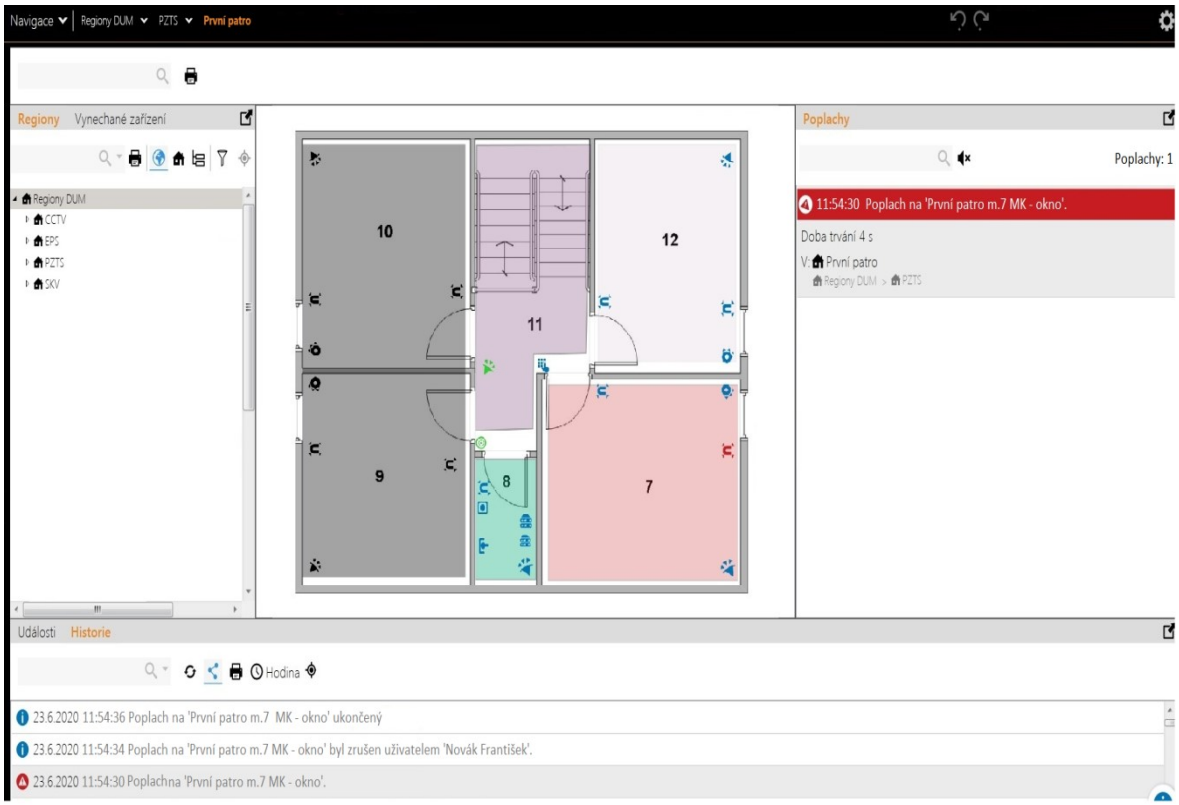
do PZTS systému můžeme využít dvě možnosti. Buďto naše vytvořená tlačítka, nebo rolovacího menu vyvolané přes šipku umístěnou za názvem Regiony DUM, kde je možné vybrat specifický systém, jak je také patrno z obrázku 36.

Po vybrání našeho sytému tedy PZTS se mapa přepne do další úrovně obr. 37, kde si vybereme požadované patro. Pro tento účel si zvolíme první patro. Opětovně můžeme pro další přepnutí mapy využít jak odkazového prvku „polygon“ umístěného v prostoru prvního patra, tak opět za zvolit rolovací menu. Ostatní systémy, jako je EPS, CCTV, SKV jsou k dispozici pro ostrahu v úplně stejném postupu a pro každý systém se otevře konečná mapa s příslušnými prvky daného systému.

Obr. 37 Zobrazení možností výběru pater

Na obrázku 38 je pak vidět náš hledaný výsledek. Zobrazí se mapové schéma pro první patro systému PZTS. Na něm je vidět rozmístění prvků PZTS v prvním patře a zároveň i zabezpečené zóny pro dané patro. Pro přehlednost jsou zde nasimulovány i veškeré možnosti, které systém umožnuje. Obsluhu má díky jednoduchému barevnému rozlišení přehled, co se na objektu děje. V místnosti dvanáct, jak je vidět na našem obrázku jsou veškeré prvky neaktivní, a proto zóna zabezpečení je světlé barvy. To znamená, že se daná zóna muže kdykoliv bez potíží ihned zastřežit. V místnosti jedenáct má zóna tmavší odstín a je v ní jeden prvek aktivní. Jedná se o PIR detektor, který má zelenou barvu. Každý aktivní prvek je znázorněn touto barvou. Pokud je prvek neaktivní tedy není spuštěn má modrou barvu. Zóna se dá totiž zastřežit pouze v případě, že PIR bude neaktivní anebo bude případně vynechán (inhibitován). Aktivní prvek blokuje možnost zastřežit zónu. V místnostech deset a devět jsou prvky černé i se zónou zabezpečení. To značí poruchu komunikace s prvky v této zóně. Proto je nutné začít zjišťovat příčinu nefunkční

komunikace a případně odstranit, pokud je to možné závadu bez nutnosti volat servisní firmu. Místnost osm je vybarvena zelenou barvou a tím je znázorněna zóna, která je zastřežena. Můžeme si všimnout, že světelná signalizace je též ve stavuzastřeženoa má zelenou barvu. V poslední místnosti číslo sedmu je vyvolán poplach na magnetickém kontaktu okna. Každá vyvolaný poplach prvkem v objektu, je znázorněn červenou barvou, jako je tomu na obrázku níže. Pokud se tak stane v pravé části v okně, vyskočí informační událost o daném poplachu a v událostech či historii se ukazuje průběh daného poplachu. V našem případě je vidět na obrázku níže, že po vzniku poplachu pan Novák tento poplach zrušil a ukončil. Pokud má prvek žlutou / oranžovou barvu je v poruše.



Obr. 38 Grafické schéma budovy s bezpečnostními prvky

Operátor má v zásadě několik možností, jak naložit se vzniklým poplachem. První byla ukázána na obrázku, kdy je poplach odbaven s tím, že to byl ojedinělý incident zapříčinění například zakolísáním napětí v systému a již se neopakuje. Druhá možnost je potvrzení poplachu a vynechání prvku, jenž je neustále v poplachu například z důvodu otevřeného okna. Pokud by se tak neučinilo, byl by po potvrzení tohoto poplachu opětovně poplach vyvolán. V každém případě u první či druhé možnosti je vždy nutné prověřit na místě ostrahou důvod poplachu. Nicméně lze využít i možnosti například kontrolního telefonního hovoru se subjektem, který je přímo na místě události a dotázat se na situaci. Také je

možné, pokud to instalace dovoluje použít k identifikaci příčiny poplachu kamerového záznamu. Tímto, bychom mohli uzavřít celou fázi našeho projektu, jenž měl poukázat na možnosti moderních softwaru k zajistit bezpečnost našich domovů a životů prostřednictvím integračních aplikací a grafických vizualizací, které tyto softwary v dnešní době poskytují pro své uživatele.

4 BUDOUCNOST V TOMTO ODVĚTVÍ

Budoucnost těchto systémů má velký potenciál a vzhledem k novým inovacím se tento model bude nadále rozvíjet. Již dnes je určitou snahou firem implementovat do těchto systému novinky, například takzvaný Lidar (Light Detection and Ranging). Jde o zařízení využívající laserových paprsků k mapování okolního prostoru. První aplikace tohoto zařízení byla využita sice v jiném odvětví (automobilovém), ale jeho detekční schopnosti jsou dobře aplikovatelné i pro zabezpečovací systémy. K mapování prostoru využívá principu výpočtů doby odraženého paprsku, například starší typ Velodyne VLP 16 disponuje šestnácti laserovými paprsky pro detekci. Dnes je tento počet detekčních laseru překonán a Lidar muže byt vybaven například 128 detekčními lasery, což má za následek velmi přesné a spolehlivé detekční vlastnosti. V mnoha ohledech by dokázal nahradit i zaběhnuté zabezpečovací detektory jako PIR detektor, magnetický kontakt apod. Dalším běžným prvkem bude mapování celého střeženého prostoru či objektu do 3D perspektivy. Například již zmíněny bezpečnostní systém Accur8vision v této kategorii si klade za cíle přinést nový pohled na možnost zabezpečení. Vytváří kompletní 3D mapy objektů a za pomoci moderních technologií prostřednictvím využití dronů. Dron nasnímá mapu objektu za pomoci například zmíněného Lidaru a vytvoří tím obrovské množství bodů zvaných Point Cloud. Tyto body jsou zpracovány softwarem a s pomocí fotogrammetrie, jenž přidá bodům i barvu aplikace vytvoří 3D mapu. Vzniká tím jedineční poziční systém, který lze, pokud je zapotřebí i modulovat. V této mapě je poté každý detektor či kamera přesně umístěna a díky pozičnímu systému lze snadno odhalit i hluchá místa kam by detektor případně kamera nebyly schopny pokrýt z důvodu terénu. A to vše lze zjistit ještě před zahájením samotné instalace. Budoucnost v tomto oboru bude velice zajímává a dočkáme se v blízké době velice zajímavých řešeních a nových technologiích, které se budou starat o naši bezpečnost na každém našem kroku v životě.

ZÁVĚR

Oblast bezpečnostní technologie je v dnešní době velice rychle se rozvážející a dynamický obor. Technologický pokrok, jehož bylo dosaženo v několika dekádách nám dnes zajišťuje pocit většího bezpečí a ochranu majetku či zdraví. Bezpečnost je lépe zajištěna prostřednictvím například nových softwarových aplikací, konkrétně v této práci prostřednictvím integračního nástroje C4 od firmy Gammanet propojujícího různé druhy systémů. Díky jednoduchému a přehlednému zobrazení je pak pro obsluhu takového sytému usnadněna kontrola hlídané oblasti, a tím zajištění i kvalitnější ochrany. Také prostřednictvím této práce si muže laická veřejnost snadno udělat obrázek na jakém principu pracují dnešní programy v této oblasti a zařízení zajištující jejich nepřetržité bezpečí.

SEZNAM POUŽITÉ LITERATURY

[1]LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I*. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 81 s. ISBN 9788073188894.

[2]LAUCKÝ, Vladimír. *Speciální bezpečnostní technologie*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 223 s. ISBN 9788073187620.

[3]BRABEC, František. *Technologie detektivních činností*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 160 s. ISBN 9788073187804.

[4]VALOUCH, Jan. *Projektování integrovaných systémů*. Vydání druhé. Zlín: Univerzita Tomáše Bati ve Zlíně, 2015, 1 online zdroj (169 stran). ISBN 9788074545573. Dostupné také z: http://hdl.handle.net/10563/18616

[5] IVANKA, Ján. *Systemizace bezpečnostního průmyslu*. Vyd. 5. Ve Zlíně: Univerzita Tomáše Bati ve Zlíně, 2014, 219 s. ISBN 9788074544101. Dostupné také z: http://hdl.handle.net/10563/27488

[6]LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management: [teorie a praxe ochrany majetku a fyzické bezpečnosti]*. 3. vyd. Zlín: VeRBuM, 2013, 456 s. ISBN 9788087500057.

[7] TRADE FIDES, a.s. Trade FIDES, a.s. LOW X. LatisOperator Workstation Pracoviště výkonného operátora. Manuál uživatele systému. *DOCPLAYER* [online]. [cit. 2020-04-08]. Dostupné z: view-source:https://docplayer.cz/17497056-Trade-fides-a-s-low-2-2-0-x-latis operator-workstation-pracoviste-vykonneho-operatora-manual-uzivatele-systemu.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CCTV Uzavřený kamerový systém

DPPC Dohledové poplachové přijímací centrum

EPS Elektrická požární signalizace

GB Detektor tříštění skla (Glass Break)

MK Magnetický kontakt

OTD Otřesový detektor

PIR Pohybový infračervený detektor pohybu.

PZTS Poplachový tísňový a zabezpečovací sytém

SKV Systém kontroly vstupu

SEZNAM OBRÁZKŮ