Integrace poplachových systémů s využitím prvků informačních technologií

Integration of alarm systems using elements of information technology

Bc. Tomáš Macháč

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

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

Jméno a příjmení:	**Bc. Tomáš MACHÁČ**
Osobní číslo:	**A11291**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Integrace poplachových systémů s využitím prvků informačních technologií**

Zásady pro vypracování:

1. **Analyzujte legislativní a technické požadavky na integraci poplachových systémů.**
2. **Specifikujte současné technické možnosti integrace poplachových systémů s využitím prvků informačních technologií.**
3. **Na modelovém objektu navrhněte integrovaný poplachový systém.**
4. **Pojednejte o vývojových trendech konvergence poplachových a informačních technologií.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **VALOUCH, Jan. Projektování bezpečnostních systémů. [skriptum]. Zlín: UTB, 2012. ISBN 978-80-7454-230-5. 152 s.**
2. **VALOUCH, Jan. Integration Techniques of Alarm Systems. In TRANSACTIONS of the VŠB – Technical University of Ostrava. Ostrava: VŠB, 2012. No. 1, Vol. VII. Safety Engineering Series. p. 65-72. ISSN: 1801-1764.**
3. **VALOUCH, Jan. Bezpečnostní technologie, systémy a management. 1.vyd. Luděk LUKÁŠ. Zlín: VeRBuM, 2011. ISBN 978-80-87500-05-07. Legislativní rámec projektování zabezpečovacích systémů, s.171-183.**
4. **ČSN CLC/TS 50398. Poplachové systémy- Kombinované a integrované systémy- všeobecné požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. 20 s. Třídící znak 334597.**
5. **HERMANN, Merz, THOMAS, Hansemann a CHRISTOF, Hübner. Automatizované systémy budov: Sdělovací systémy KNX/EIB, LON a BACnet. Praha: Grada, 2009. Edice Stavitel. 264 s. ISBN 978-80-247-2367-9.**
6. **VALEŠ, Miroslav. Inteligentní dům. 1. vyd. Brno: ERA, 2006. 123 s. ISBN 80-7366-062-8.**

Vedoucí diplomové práce: **Ing. Jan Valouch, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **8. února 2013**

Termín odevzdání diplomové práce: **3. června 2013**

Ve Zlíně dne 8. února 2013

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato práce pojednává o využití prvků informační technologie v integraci poplachových systémů. V první kapitole je rozebrána problematika, která představuje analýzu legislativních a technických požadavků na prvky, které jsou využity při integraci poplachových systémů. Následující část pojednává o současné možnosti integrace poplachových systémů, kde je popsána struktura, funkce a komunikační propojení jednotlivých subsystému. Hlavním výstupem této práce je praktická část, která zpracovává konkrétní návrh integrovaného poplachového systému pro výrobní objekt. Závěr obsahuje vývojové trendy v oblasti integrací poplachových systémů.

Klíčová slova: integrovaný poplachový systém, integrace, komunikace, informační technologie, informace, přenosová rychlost, kruhová topologie.

ABSTRACT

This work deals with use of elements of information technology in the integration of alarm systems. Beginning of this thesis presents an analysis of legislative and technical requirements for the elements used in the integration of alarm systems. This analysis includes the possibility of integrating this moment in alarm systems, which describes the structure, function and connection of individual communication subsystem. The central output of work is in the practical part of the integrated design process concrete alarm system for financial institutions. In conclusion we suggest trends for the integration of elements.

Keywords: integrated alarm system, integration, communication, information Technology, information, transmission rate, ring topology.

„Vzdělání má hořké kořínky, ale sladké ovoce.“

Aristotelés

Rád bych touto cestou poděkoval svému vedoucímu diplomové práce panu Ing. Janu Valouchovi, Ph.D. za odborné vedení, rady a věcné připomínky, které mi poskytoval v průběhu zpracování celé práce.

Za odbornou pomoc bych chtěl poděkovat svému kolegovi z práce, panu Petru Sedlaříkovi – technik v bezpečnostní firmě. Za další odborné znalosti, které mi pomohly ke zpracování diplomové práce, chci poděkovat technickému řediteli METEL s.r.o. Tomáši Metelkovi.

V poslední řadě bych chtěl poděkovat i své nejbližší rodině a mé přítelkyni za morální i finanční podporu během celého studia na Fakultě aplikované informatiky UTB ve Zlíně.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/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 diplomová/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 diplomovou/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 s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/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 diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

V současné době existuje velké množství poplachových systémů, které lze instalovat v nejrůznějších objektech. Od běžných rodinných domů, přes průmyslové budovy až po bankovní instituce. Snad každý majitel objektu očekává od instalovaných systémů bezporuchový provoz a spolehlivost zabezpečení.

Ve většině počátku realizace poplachových systémů dochází často k chybě v samotném zadání zakázky. Dochází zde k problému ve vzájemné komunikaci mezi bezpečnostní firmou a majitelem objektu, kdy firma z důvodu cenové konkurenceschopnosti nabízí levnější systémy, které se ale v průběhu využívaní ukážou jako nevhodné. Důležitým faktorem mohou být vysoké náklady při prvotním provedení integrovaného systému.

Pokud si majitel objektu postupem času přeje rozšířit stávající systém o nové funkce, následkem může být funkční neschopnost systému, která může vést k výskytu následných provozních problémů. Zásah do rozsáhlých instalovaných systémů se může jevit jako problém, jak pro montážní firmy, tak pro majitele. Důvodem je nefunkčnost zabezpečení objektu po dobu nezbytně nutnou při nutné úpravě systému.

Bezpečnostní firmy by proto měly při prvotní konzultaci s majitelem objektu projednat výhody integrovaných systémů. Propojení poplachových aplikací:

- poplachové zabezpečovací a tísňové systémy (PZTS),
- systém kontroly vstupu (ACS),
- uzavřený televizní okruh pro bezpečnostní aplikace (CCTV),
- systém přivolání pomoci (SAS),
- elektrická požární signalizace (EPS),

nám přináší spoustu výhod do budoucna. Jednou z výhod je například účinné sledování přístupu osob do jednotlivých částí objektu, vyšší přínos informací o bezpečnostní situaci objektu, centralizovaná obsluha nad instalovanými systémy nebo také možnost přenosu informace kontroly docházky zaměstnanců na mzdový systém. Integrovaný poplachový systém splňuje možnost efektivního rozšíření do budoucna o další prvky.

S poplachovými aplikacemi lze integrovat i nepoplachové aplikace, které nemají ve své primární funkci ochranu života a majetku.

Propojením nepoplachových aplikací:

- osvětlení,
- správa energetiky,
- klimatizace, topení,
- řízení výtahů,
- správa budovy,

nám přináší spoustu výhod jak už z hlediska snížení ekonomické náročnosti provozu, tak zvýšením komfortu využívaní systému pro uživatele.

Tato práce se zaměřuje na zabezpečení průmyslových budov. Důvodem je rozlehlost budov, se kterou jsou spojeny i větší požadavky na kabeláž a na množství akčních prvků na komunikační trase. Průmyslový objekt v této práci bude administrativní budovu se sousedící výrobní halou, na které budou prezentovány současné možnosti propojení více subsystému do jednoho integrovaného systému. Integrovat lze v dnešní době skoro všechny systémy. Důležitým faktorem spolehlivého provázání funkčnosti jednotlivých systémů je vzájemná komunikace. Tato komunikace musí probíhat pomocí standardizovaných protokolů, které předcházejí špatné a kolizní komunikaci mezi systémy.

Propojení poplachových systémů bude nastíněno v analytické části diplomové práce. Výsledkem práce bude návrh integrovaného poplachového systému, který bude pro komunikaci využívat prvky informační technologie.

I. TEORETICKÁ ČÁST

1 LEGISLATIVNÍ POŽADAVKY

V České republice jsou obecně závazná pravidla chování stanovena předepsanou morálkou státní moci, které jsou zakotvena v závazných právních normách, zvaných obecně právní předpisy. Soubor právních předpisů tvoří právní řád státu. Nejvyšším právním aktem psaného práva je zákon. Dále Česká republika je závazně upsaná mezinárodním smlouvám. Nižší právní sílů prezentují nařízení vlády a vyhlášky, vydány k příslušným zákonům, určují podrobnosti o povinnostech a právech. Nařízení vlády a vyhlášky nesmí překročit rámec příslušných zákonů [1].

V právním řádu jsou obsaženy ustanovení, která řeší rovněž problematiku vztahující se k nasazení integrovaných poplachových systémů.

Jednotlivé oblasti právních ustanovení udávají požadavky na:

- ochranu utajovaných informací,
- prevenci vzniku havárie,
- zabezpečení,
- projektování staveb,
- výstavbu staveb,
- dokumentaci,
- výrobek a elektrická zařízení,
- odbornou způsobilost,
- bezpečnostní politiku organizace.

Trendem v dnešní době je stavba velkých center, se kterými je následně spojen výskyt velkého počtu lidí na jednom místě. Proto je nutné brát v potaz i elektrickou požární signalizaci, která v legislativě svými stanovisky ovlivňuje široké spektrum účastníků průběhu stavby nové budovy.

1.1 Ochrana osobních údajů

Tato podkapitola se zabývá ochranou a zpracováním osobních údajů, které jsou nedílnou součástí jakéhokoliv záznamu v informačním systému, kamerovém záznamovém zařízení, přístupovém a docházkovém systému, mzdovém softwaru a osobních dokladech.

Tyto stanoviska osobních údajů v rámci České republiky nařizuje zákon č. 101/2000 Sb., o ochraně osobních údajů. Tento zákon vychází ze směrnice Evropského parlamentu a Rady 95/46/ES z 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Směrnice vytyčila oblasti zpracování osobních údajů:

- archivnictví, bankovnictví, daňové řízení, doprava, katastr nemovitostí,
- e-government, elektronická komunikace, matrika a notáři,
- kamerové systémy, kasina, pojišťovnictví, policejní postupy,
- pracovněprávní vztahy, rodná čísla, sociální zabezpečení, školství
- statistická zjišťování, školství, volby, zdravotnictví [2].

Z hlediska poplachových aplikací se bude jednat o systém kontroly přístupu a kamerové systémy. Pro kamerové systémy je obsažen výčet různých právních stanovisek, která se týkají zpracováním osobních údajů a nasazení kamerových systémů:

- zákon č 273/2008 Sb., o Policii České republiky,
    - oprávnění Policie České republiky k pořizování zvukových, obrazových nebo jiných záznamů,
- zákon č. 553/1991 Sb., o obecní policii,
    - oprávnění obecní policie k pořizování zvukových, obrazových nebo jiných záznamů,
- zákon č. 262/2006 Sb., zákoník práce,
    - zákaz podrobovat zaměstnance otevřenému nebo skrytému sledování bez závažných důvodu spočívajícího ve zvláštní činnosti zaměstnavatele,
- zákon č. 129/2008 Sb., o výkonu zabezpečovací detence a o změně některých souvisejících zákonů,
    - oprávnění trvale sledovat chovance s využitím kamerového systému,
    - kontrola chovance, vůči němuž byly omezovací prostředky použity po delší dobu, s využitím kamerového systému,
- zákon č. 109/2002 Sb., o výkonu ústavní výchovy nebo ochranné výchovy ve školských zařízeních a o preventivně výchovné ve školských zařízeních a o změně dalších zákonů,
    - audiovizuální systémy a možnost jejich využití,
- zákon č. 202/1990 Sb., o loteriích a jiných podobných hrách,

- povinnost kasina být vybaven kamerovým systémem, pro podmínky provozu tohoto zařízení [3].

Stěžejním zákonem v ochraně osobních údajů v ČR je zákon č. 101/2000 Sb., o ochraně osobních údajů. Zákon se vztahuje na osobní údaje, které jsou zpracovány státními orgány, orgány územní samosprávy a dalšími orgány veřejné moci, také ale i fyzickýma a právnickýma osobami. Dále se vztahuje na veškeré zpracovávání osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky. Nevztahuje se na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu. Také se zákon nevztahuje na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány. Zákon se vztahuje na zpracování osobních údajů v rámci statistiky a archivnictví.

Zákon o ochraně osobních údajů vymezuje následující pojmy:

osobní údaj – jakýkoli údaj týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za jednoznačný, jestliže lze na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu. O osobní údaj se nejedná, pokud je ke zjištění jeho identity použito nepřiměřené množství času, úsilí i materiálních prostředků,

citlivý údaj – jedná se o osobní údaj vypovídající o národnosti, rasovém nebo etnickém původu, politických postojích, členství výborových organizacích, náboženské a filozofické orientaci, trestné činnosti, zdravotním stavu a sexuálním životě subjektů údajů,

anonymní údaj – takový údaj, který buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout na jakýkoliv subjekt,

subjekt údajů – fyzická osoba, k níž se vztahují osobní údaje,

zpracování osobních údajů – operace nebo soustava operací, které správce nebo zpracovatel systematicky provádí s osobními údaji, a to automatizovaně nebo pomocí jiných prostředků. Zpracováním údajů se rozumí shromaždování, ukládání na nosiče informací, zpřístupňování, úprava nebo změna, vyhledávání, používání, předávání, šíření, zveřejňování, výměna, uchovávání, třídění, kombinování, blokace a likvidace.

správce – subjekt, který určuje prostředky a účel zpracování osobních údajů, provádí zpracování a zodpovídá za něj. Zpracováním osobních údajů může správce pověřit nebo zmocnit zpracovatele[2].

Práva a povinnosti při zpracování osobních údajů, jsou kladeny jak na správce, tak i na pověřeného zpracovatele. Správce je povinen:

- stanovit účel, k němuž mají být osobní údaje dále zpracovány,
- stanovit prostředky a způsob jakým budou zpracovány osobní údaje,
- zpracovávat pouze pravdivé a přesné údaje. Správce je povinen ověřovat pravdivost údajů. Nepravdivé, nepřesné nebo neověřené údaje, lze zpracovávat pouze v případě stanoví li zvláštní zákon,
- shromažďovat osobní údaje odpovídající pouze stanovenému účelu,
- uchovávat údaje po dobu nezbytně nutnou k jejich zpracování. Po uplynutí této doby mohou být údaje uchovány pouze pro účely statistické, vědecké a archivnictví.

Správce je před zahájením zpracování osobních údajů povinen subjekt údajů řádně a včas písemně vyrozumět o tom, v jakém rozsahu a pro jaký účel budou údaje zpracovány. Kdo a jakým způsobem bude údaje zpracovávat a komu mohou být zveřejněny, či komu jsou určeny [2].

1.2 Požárně bezpečnostní aspekty

Požární bezpečnost je jedna z hlavních a výchozích vlastností objektu. Zahrnuje široké spektrum účastníků podílejících se na požárně bezpečnostních aspektech objektu. Od tvůrce zákonů a vyhlášek, přes projektanty, servisní firmy, až po uživatele využívající objekt.

Prioritou vytváření a rozvíjení podmínek požární bezpečnosti je ochrana života a zdraví občanů, snížení škody způsobené na majetku a pomoc při mimořádných událostech.

Strategie požární bezpečnosti obecně vychází z ustanovení Zákona č. 133/1985 Sb., o požární ochraně ve znění pozdějších předpisů.

Ostatní činnosti spjaté s provozem, montáží, údržbou a úpravami věcných prostředků požární ochrany a požárně bezpečnostních zařízení jsou řízeny dalšími požadavky na kvalifikační a odborné znalosti osob vykonávající tyto úkoly.

Zákon č. 133/1985 Sb., o požární ochraně, ve znění pozdějších předpisů

Základním účelem zákona je vytvořit podmínky pro účinnou ochranu života, osob a majetku před vznikem požárů. Zákon stanovuje podmínky při poskytování pomoci v ochraně před mimořádnou událostí a to stanovením povinností ministerstev a jiných správních úřadů,

právnických a fyzických osob. Dále udává postavení orgánů státní správy a samosprávy na úseku požární ochrany a upravuje povinnosti jednotkám hasičského záchranného sboru.

Důležitý faktor požární ochrany je dodržováním zásad a povinností. Tyto povinnosti jsou kontrolovány pomocí výkonu státního požárního dozoru, jenž vykonává:

- kontrolu dodržování povinností orgánů státní správy, právnických osob a podnikajících fyzických osob, stanovených předpisy o požární ochraně
- posuzování územně plánovací dokumentace staveb a technologií z hlediska požární bezpečnosti
- ověřování zda byly dodrženy podmínky požární bezpečnosti staveb, vyplívající z podkladů a dokumentace
- posuzování výrobků, které nebyly určeny ke schvalování státním zkušebnám, z požární bezpečnosti
- schvalování posouzení požárního nebezpečí činností, u nichž hrozí vzniku požárů
- zjišťování příčin vzniku požáru
- kontrolu připravenosti a akceschopnosti jednotek požární ochrany
- ukládání opatření k odstranění zjištěných nedostatků a kontrolou plnění těchto opatření [4].

Zákon č. 183/2006 Sb., o územním plánování a stavebním úřadu (stavební zákon)

Oblast zabývající se elektrickou požární signalizací ve stavebním zákoně se zaměřuje na požadavky na výrobky a konstrukční materiál použity na stavbě. Materiál musí splňovat zátěžové zkoušky na mechanickou odolnost. Při pravidelné údržbě a kontrole je zaručena dlouholetá stabilita použitého materiálu, který nebude ohrožovat zdraví lidí, znečištění přírody a šíření hluku. Požární bezpečnost budovy, musí splňovat odolnost materiálů po dobu nutnou k ochraně lidí a zvířat.

Vybrané činnosti ve výstavbě, jejichž výsledek ovlivňuje ochranu veřejných zájmů, mohou vykonávat pouze fyzické osoby, které získaly kvalifikační oprávnění k výkonu činností podle zákona č. 360/1992 Sb., o výkonu povolání autorizovaných architektů a o výkonu povolání autorizovaných inženýrů a techniků činných ve výstavbě, ve znění pozdějších předpisů. Za vybrané činnosti se podle stavebního zákona považuje:

- projektová činnost ve výstavbě, kterou se rozumí zpracování územně plánovací dokumentace, územní studie, projektová dokumentace pro vydání stavebního

povolení, dokumentace pro vydání územního rozhodnutí, projektová dokumentace pro ohlašování stavby, provádění stavby a nezbytné úpravy,

- odborné kvalifikační znalosti k provádění a řízení stavby nebo její nezbytné úpravy [5].

Vyhláška č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci)

Ministerstvo vnitra ČR v roce 2001 vydalo vyhlášku č. 246/2001 Sb., o požární prevenci, která rozšiřuje povinnosti účastníků požární ochrany vztahující se k zákonu č. 133/1985 Sb., o požární ochraně.

Ve vyhlášce je důležité se zaměřit na problematiku zabývající se projektováním požárně bezpečnostních zařízení. Dále vyhláška pojednává o požadavcích na projektování, montáž a kontrolu provozuschopnosti požárně bezpečnostních zařízení a hasicích přístrojů. Obsah a rozsah požárně bezpečnostního řešení je uvedeno přesně ve vyhlášce. Jeden ze způsobu státního požárního dozoru je tzv. požární prevence, která je v požární ochraně nejdůležitější.

Při posuzování dokumentace staveb a technologií se zjišťuje:

- bezpečná evakuace všech osob a zvířat do bezpečného prostoru,
- časové zachování stability a nosnosti konstrukcí budovy po určitou dobu,
- stanovení požárně bezpečnostních zařízení,
- rozdělení objektů do jednotlivých požárních úseků, vymezení požárně nebezpečného prostoru,
- zabránění šíření požárů a vzniklých zplodin,
- stanovení požárního rizika,
- druhy konstrukcí posle požární odolnosti,
- vymezení zásahových, příjezdových a evakuačních cest,
- vybavení objektu věcnými prostředky pro potlačení požáru [6].

Vyhláška č. 23/2008 Sb., o technických podmínkách požární ochrany stavby

Tato vyhláška se zabývá problematikou stanovení technických podmínek požární ochrany pro navrhování, provádění a užívání stavby. Stanovuje i stupeň požární bezpečnosti, což je schopnost stavebních konstrukcí požárního úseku jako celku odolávat působením požárů

z hlediska možného rozšíření požáru a stability konstrukce stavby. Stupeň požární bezpečnosti se určuje podle českých technických norem podle druhu stavby v závislosti na:

- požárním riziku,
- konstrukčním provedením stavby,
- výška budovy, počet podlaží.

Stavba musí být navržena a umístěna tak, aby splňovala podle druhu technické podmínky požární ochrany, zabývající se:

- požárně nebezpečným a bezpečným prostorem,
- zdrojem požární vody a ostatního hasiva,
- přístupovou komunikací a nástupní plochou požární techniky,
- zabezpečením stavby, jednotkami požární ochrany.

Pří navrhování stavby musí být splněny technické podmínky požární ochrany zaměřené na:

- stavební konstrukce
- technologická zařízení
- evakuace osob a zvířat [7].

Základní normy požárního kodexu

Hlavní postupy požární bezpečnosti staveb jsou řešeny otevřeným souborem norem, který nazýváme požární kodex. Požadavky, které stanovují závazné právní předpisy (zákony a vyhlášky), jsou dále rozpracovány ještě dalšími technickými požadavky, předpisy a normami. Oblasti navrhování a projektování elektrické požární signalizace je systematicky rozebráno v následujících ČSN třídách.

- Třída 34 – Elektrotechnika
    - **ČSN EN 54 - 1 – 25** Elektrická požární signalizace – požadavky na ústřednu, napájecí zdroj, hlásiče, přenosová zařízení atd.,
    - **ČSN EN 34 27 10** Elektrická požární signalizace – projektování, montáž, užívání, provoz, kontrola, servis a údržba.
- Třída 38 – Energetika – požární bezpečnost
    - **ČSN EN 38 01 - 38 98** Energetika – Třída norem ukládající požadavky od výstavby elektráren, bezpečnostních značek, hasicí vozy, prevence a ochrana proti výbuchu, kabelové rozvody, přepěťové ochrany atd.

- Třída 73 – Navrhování a provádění staveb

  Stěžejní normou požární bezpečnost staveb je třída norem ČSN EN 7308xx, kde hlavním předpokladem navrhování požární bezpečnosti staveb je míra požárního rizika. S tím jsou spjaté příčiny negativního vzniku požáru, jeho šíření a minimalizace vzniklých škod.

  Jednotlivé normy se vztahují na výrobní a nevýrobní objekty, zdravotnická střediska, shromažďovací prostory, zemědělské objekty, sklady, zásobování požární vodou atd.

  - **ČSN EN 73 0875** Požární bezpečnost staveb – stanovení podmínek navrhování elektrické požární signalizace v rámci požárně bezpečnostního řešení [8].

1.3 Požadavky na výrobky

Chceme-li docílit spolehlivého a plně funkčního integrovaného poplachového systému, je třeba při jeho realizaci používat výrobky, které jsou svým způsobem bezpečné pro své okolí v místě nasazení. Obecnou problematiku bezpečnosti výrobku upravuje Zákon č. 102/2001 Sb. o obecné bezpečnosti výrobků a o znění některých zákonů, které stanovují základní právní požadavky na výrobce, dovozce a distributory [9].

Tento zákon zastřešuje další právní předpisy, které jsou nezbytné k posouzení výrobku na trhu.

Zákon č. 22/1997 Sb., o technických požadavcích na výrobky

Při navrhovaní a realizaci jakéhokoliv systému nebo zařízení, je nutné pro efektivní uspokojení potřeb používat výrobky testované příslušným certifikačním orgánem. Výrobek musí splňovat ES prohlášení o shodě, kde je ověřována shoda vlastností a technických parametrů výrobku s požadavky technických norem a právních předpisů, potřebných k prokázání shody. Všechny výrobky při uvedení na náš trh musí splňovat požadavky kladené zákonem č. 22/1997 Sb. o technických požadavcích na výrobky. Tyto požadavky se vtahují na výrobce, dovozce a distributory.

Při **posuzování bezpečnosti výrobku** se berou v úvahu faktory životnosti výrobku, vlastnosti, složení balení, návody (montážní, uživatelské, likvidační), vliv výrobku na ostatní zařízení a zařazení do věkové kategorie uživatelů. Tyto aspekty předcházejí rizikové

manipulaci a vzniku ohrožení zdraví, osob, majetku nebo životního prostředí. Aspekty ovlivňující skupinu požadavků na výrobek se označuje oprávněným zájmem.

Tento zákon vymezuje výrobky, které mohou ohrozit svým nebezpečným chováním oprávněný zájem. Pro tyto výrobky vydává tzv. obecné povinnosti, které označují jako výrobky stanovené. Výrobcům i dovozcům jsou v této souvislosti ukládány dvě **základní povinnosti**:

- **zajistit** posouzení shody vlastností stanovených výrobků postupem, který je stanoven odpovídajícím prováděcím předpisem,
- **vydat** prohlášení, že shoda výrobku byla posouzena postupem stanoveným odpovídajícím právním předpisem [10].

Za stanovené výrobky se považují i výrobky, které jsou na náš trh uváděny jako použité nebo repasované. Českou značku shody obsahuje výrobek, který splnil požadavky stanoveným tímto zákonem [11].

Nařízení vlády č. 17/ 2003 Sb., kterým se stanoví technické požadavky na elektrická zařízení nízkého napětí.

Tímto nařízením se stanoví technická ustanovení požadavků na elektrická zařízení nízkého napětí.

Elektrickým zařízením se rozumí jakékoliv zařízení určené pro použití v rozsahu jmenovitého napětí od 50 V 1000 V pro střídavý proud a jmenovitého napětí od 75 V do 1500 V pro stejnosměrný proud.

Elektrické zařízení může být uvedeno na trh, jestliže splňuje požadavky stanovené tímto nařízením a neohrožují při správné instalaci bezpečnost obyvatel, zvířat a majetku. Prokázání bezpečnosti elektrických zařízení je vydání dané shody.

Posouzení shody u elektrického zařízení je opatřeno označením CE a vydá ES prohlášení o shodě, které musí obsahovat:

- identifikační prvky o výrobci nebo zplnomocněném zástupci,
- identifikační údaji o distributorovi a prodejci,
- podrobný popis elektrického zařízení,
- odkaz na soubor harmonizovaných norem,
- specifikace, na jejichž základě byla provedena shoda,

- poslední dvojčíslí roku, kdy bylo vydáno označení CE zařízení.

Technické **požadavky** všech elektrických zařízení uvedených na náš trh musí splňovat:

- všeobecné požadavky
- ochranu před nebezpečím, které může elektrické zařízení způsobit,
- ochranu před nebezpečím, které mohou vzniknout působením vnějších vlivů,
- soulad se správnou technickou praxí ve výrobě elektrického zařízení,
- bezpečný provoz elektrického zařízení, tak aby neohrozilo při správné instalaci, údržbě a používání bezpečnost osob, domácích a hospodářských zvířat nebo majetek [12].

Nařízení vlády č. 616/2006 Sb., o technických požadavcích na výrobky z hlediska jejich elektromagnetické kompatibility

Všechny technické požadavky na zařízení týkající se elektromagnetické kompatibility jsou stanoveny Nařízením vlády č. 616/2006 Sb., o technických požadavcích na výrobky z hlediska jejich elektromagnetické kompatibility.

Česká republika přijala mezinárodní směrnici v rámci členských státu EU, jedná se o Směrnici Evropského parlamentu a rady 2004/108ES o sbližování právních předpisů týkající se elektromagnetické kompatibility.

Nařízení vlády 616/2006 Sb. upřesňuje podrobnosti v základních technických požadavcích na výrobky, na postup posuzování shody zařízení a stanovení podmínek pro autorizace právnické osoby.

Požadavky na výrobky v oblasti elektromagnetické kompatibility musí být stanoveny tak, aby použité zařízení:

- nepřekročilo příslušnou úroveň elektromagnetického rušení (interference), tak aby ovlivnilo stanovenou funkci dalších zařízení,
- vykazovalo příslušnou odolnost vůči elektromagnetickému rušení (susceptibility) v místě použití zařízení, předcházelo nepřijatelnému stavu funkce.

Ve smyslu toho nařízení vlády 616/2006 Sb. se zařízení používá pro:

- pevnou instalaci – soubor několika druhů zařízení a jiných přístrojů, jejichž instalace je realizována na předem stanovené místo,
- mobilní instalaci - soubor několika zařízení a jiných zařízení, umožňující svou konstrukcí a provedením použití na různých místech [13].

Nařízení vlády č. 426/2000 Sb., kterým se stanoví technické požadavky na radiová a na telekomunikační koncová zařízení

Tímto Nařízením vlády č. 426/2000 Sb. se kladou podmínky na bezdrátový i drátový přenos informace. V bezpečnostní praxi se kladou podmínky na GSM moduly, které využívají stanovené frekvenční pásmo. Požadavky jsou také stanoveny na připojení ústředny k dohledovému a poplachovému přijímacímu centru pomocí jednotné telefonní sítě. Další možnost připojení je pomocí radiové sítě, která pracuje na stanovených frekvenčních pásech a spousta dalších převážně bezdrátových přenosů je regulované tímto nařízením.

Česká republika přijala po vstupu do Evropské unie Směrnici Evropského parlamentu a rady 1999/5/ES o radiových zařízení a telekomunikačních koncových zařízení a vzájemné uznávání jejich shody.

Požadavky jednotlivých zařízení jsou klasifikovány a zařazeny do určitých tříd a typů, které jsou stanoveny v Telekomunikačním věstníku Českého telekomunikačního úřadu. Mezi základní požadavky na zařízení patří:

- ochrana zdraví a bezpečnost uživatele jakékoliv další osoby, včetně cílu uvedených v Nařízení vlády č. 17/2003Sb. a to bez zřetele na hodnotu napětí,
- ochrana týkající se elektromagnetické kompatibility daná Nařízením vlády č. 616/2006 Sb.,
- rádiová zařízení musí být konstruována tak, aby efektivně využívala kmitočtové pásma přidělené pro zemskou nebo kosmickou radiokomunikaci,
- provedení konstrukce musí být provedeno tak, aby neovlivňovalo svůj i okolní interferenční obrazec.

Nařízení vlády č. 426/2000 Sb. stanovuje přesné pojmy jako:

Telekomunikační koncové zařízení, kterým se rozumí výrobek nebo jeho součást důležitá pro komunikaci, které je připojené na rozhraní veřejné telefonní sítě.

Rádiové zařízení, kterým se rozumí výrobek nebo jeho důležitá součást pro bezdrátovou komunikaci s použitím kmitočtového spektra přiděleného pro zemskou nebo kosmickou komunikaci.

Nařízení vlády se nevztahuje:

- rádiová zařízení využívaná radioamatéry,
- radiové zařízení spadající pod lodní dopravu,
- kabely a vodiče,
- zařízení určená výhradně k příjmu rozhlasového a televizního vysílaní,
- zařízení, výrobky a součástky používány v civilním letectví a řízení letového provozu,
- zařízení výlučně využívající zpravodajské služby,
- zařízení výlučně využívající Policie České republiky,
- zařízení výlučně využívající celní úřad,
- zařízení výlučně využívající ozbrojené síly České republiky [14].

1.4 Požadavky na odbornou způsobilost

Každá zainteresovaná osoba v činnosti návrhu systému, vypracování projektové dokumentace, kontrolní činnosti se podílí na celkové výstavbě integrovaného poplachového systému a musí plnit stávající právní předpisy. Každá funkce projektanta, montážního pracovníka, dodavatelské obchodní společnosti, revizního technika je ovlivňována zákony a vyhláškami, a proto znalost základních právních stanovisek by měla být samozřejmostí pro každého účastníka.

Zákon č. 360/1992 Sb., o výkonu povolání autorizovaných architektů a o výkonu povolání autorizovaných inženýrů a techniků činných ve výstavbě.

Tento zákon stanovuje požadavky a povinností na projektanty, autorizované architekty, techniky a inženýry zainteresované ve výstavbě. Dále upravuje způsob a podmínky autorizace, vznik, pravomoc a působnost České komory architektů a inženýrů a podmínky pro výkon spjaté s Evropským právem.

Vydání autorizace, představuje oprávnění fyzických osob k výkonu odborných činností ve výstavbě. Autorizace jsou pro příslušné obory, které stanovila Česká komora autorizovaných inženýrů a techniků činných ve výstavbě. Z hlediska poplachových i nepoplachových aplikací, které můžeme integrovat do jednoho systému, uděluji autorizace:

- technologická zařízení staveb,
- požární bezpečnost staveb,

- technika prostředí budov (elektrotechnická zařízení),
- městské inženýrství,
- statika a dynamika staveb,
- a ostatní, které najdou využití v lesnictví, geotechnice, vodním hospodářství, výstavba mostů a silnice [15].

Na požadavky projektantů se zde odkazuje i zákon č. 183/2006 Sb. (stavební zákon), kde projektant musí odpovídat za správnost, celistvost a úplnost svých zpracovaných materiálů, dále musí respektovat požadavky z hlediska ochrany veřejných zájmů a je povinen dbát právním předpisům.

Zákon č. 455/1991 Sb. o živnostenském podnikání

Zákon se týká každého účastníka podnikání od obchodních společností (akciová společnost, společnost s ručením omezeným, atd.), osob samostatně výdělečně činných (OSVČ) a pro všechny právnické a fyzické osoby zapsané v obchodním rejstříku.

Podnikáním se rozumí soustavná činnost provozovaná samostatně, na vlastní jméno a vlastní odpovědnost, kde hlavním cílem nedosažení stanoveného zisku a za podmínek určené k podnikání stanoveny tímto zákonem.

Podnikání v oblasti integrovaných poplachových systémů vyžaduje vlastnit koncesovanou živnost.

Pro nás budou stěžejní tyto dvě odvětví koncese:

- poskytování technických služeb k ochraně majetku a osob,
- ochrana majetku a osob [16].

Živnostenský zákon stanovuje podmínky vydávání koncesovaných listin.

Většinou jsou požadavky kladeny na dosavadní vzdělání, kde platí: čím vyšší stupeň vzdělání, tím se zkracuje doba nutné praxe.

Dále jsou stanoveny požadavky na trestní bezúhonnost všech osob spolupracující na výkonu činnosti.

Obsah koncesovaných živností musí být v souladu s ustanovením nařízení vlády č. 278/2008 Sb., o obsahových náplních jednotlivých živností [17].

U poskytování technických služeb k ochraně majetku a osob se provádí výkon činností, jako je například projektování, montáž, údržba, opravy a kontrola elektronických poplachových

systémů, určených k ochraně osob a majetku, zařízení sledující pohyby a projevy osob v objektu a jeho okolím a jiné. Patří sem i mechanické zábranné systémy a jejich následná montáž, údržba, revize a správa. Jeden ze specifických příkladů je bezpečnostní poradenství pro zvyšování standardů zabezpečení majetku a osob.

Vyhláška č. 50/1978 Sb., Českého úřadu bezpečnosti práce a Českého báňského úřadu o odborné způsobilosti v elektrotechnice

Zkoušku pro získání osvědčení dle vyhlášky musí absolvovat pověření pracovníci u obchodních společností, dále osoba podnikající jako OSVČ a všichni revizní i montážní pracovnicí.

Vyhláška je vydaná v rozsahu, který nám stanovuje stupně povinností pro jednotlivé uživatele elektronických zařízení. Elektronické zařízení je chápáno ve smyslu této vyhlášky, jako zařízení, u kterého je možné ohrožení lidského života, zdraví a majetku nebezpečným elektrickým proudem.

Uvedená vyhláška **stanovuje stupeň** odborné kvalifikace pracovníků, podmínky pro získání kvalifikačního osvědčení, ale také ukládá povinnosti organizaci a pracovníkům v souvislosti v klasifikaci.

Ověření platnosti a kvalifikovanosti vydané vyhlášky může zkontrolovat **inspektorát práce**, převážně tyto kontroly jsou prováděny při šetření nehody způsobené elektrickou energii na pracovišti.

Akreditované pracoviště provádí školení, kde výsledkem je osvědčení pro odbornou způsobilost v oborech splňující:

- § 6 vyhláška č. 50/1978 Sb. pro samostatnou činnost na elektrickém zařízení,
- § 7 vyhláška č. 50/1978 Sb. pro řízení činnosti,
- § 8 vyhláška č 50/1978 Sb. pro řízení společností a podnikání,
- § 9 vyhláška č50/1978 Sb. pro provádění revize,
- § 10 vyhláška č. 50/1978 Sb. pro samostatné projektování,
- § 11 vyhláška č. 50/1978 Sb. pro školení dalších pracovníků [18].

Dílčí závěr

Integrované poplachové systémy spadají do kategorie výrobků, které mohou ve zvýšené míře ohrozit bezpečnost a zdraví osob, majetku nebo životního prostředí. Proto se zde chci zaměřit na vybrané povinnosti firem souvisejících jak s dodávkou materiálu, tak samotnou montáži.

Na instalovaných komponentech integrovaného poplachového systému musí být „CE“ označení, udávající, že výrobek je ve shodě s příslušným Nařízením vlády 17/2003 Sb., nízké napětí; NV 616/2006 Sb., elektromagnetická kompatibilita; NV 426/2000 Sb., rádiová zařízení; NV 190/2002 Sb., stavební výrobky. Podle Nařízení vlády č. 426/2000 Sb., kterým se stanoví technické požadavky na rádiová a na telekomunikační koncová zařízení, nebo podle Směrnice Evropské rady 1999/5/ES, o rádiových zařízeních a telekomunikačních koncových zařízeních, musí navíc být u každého výrobku kopie „Prohlášení o shodě“, vystavená výrobcem, dovozcem nebo distributorem odpovědným za uvedení výrobku na trh EU.

Každý použitý výrobek, musí mít takové vlastnosti, aby byl bezpečný při výkonu své činnosti v místě jeho použití. Za výrobky odpovídá montážní firma, pro kterou je v tuto chvíli nejdůležitější Zákon č. 59/1998Sb., o odpovědnosti za škodu způsobenou vadou výrobku.

Celková elektrická instalace musí být vyhovující z hlediska bezpečnosti, což dodavatel doloží výchozí elektrickou revizi, kterou musí provádět kvalifikovaná osoba dle vyhlášky č. 50/1978 Sb., o odborné způsobilosti v elektrotechnice.

Vytvářením protipožárních podmínek pro zvýšení bezpečnosti osob a majetku je důležitým faktorem preventivní opatření vzniku požáru. Požární bezpečnost objektu musí vycházet z dostupné techniky, ale také jednotlivých požárních řádů, evakuačních cvičení a ostatních směrnic pro prevenci vzniku požáru a jeho následku.

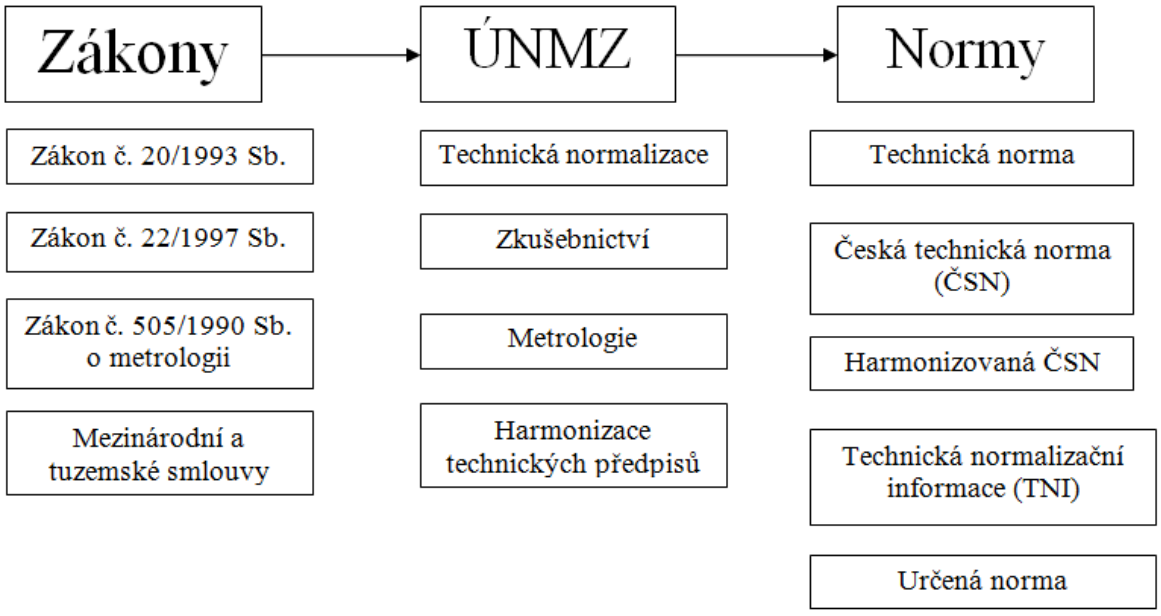
Za správnost, celistvost, úplnost a bezpečnost stavby, realizované dle projektové dokumentace a proveditelnosti stavby odpovídá projektant, který je povinen dbát právních předpisů a obecných požadavků.

2 TECHNICKÉ POŽADAVKY

Za vydávání technických norem v České republice zodpovídá úřad pro technickou normalizaci a státní zkušebnictví (ÚNMZ), který byl zřízen zákonem České národní rady č. 20/1993 Sb., o zabezpečení výkonu státní správy v oblasti technické normalizace, metrologie a státního zkušebnictví. Mezi základní poslání ÚNMZ je zabezpečovat priority vyplívající ze zákonů České republiky upravujících technickou normalizaci, metrologii a státní zkušebnictví a ostatní úkoly v rámci členství EU [19].

2.1 Normativní dokumenty

ÚNMZ vydává mimo jiné příslušené normativní dokumenty k výrobkům. Postupy uvedené v normativních dokumentech předcházejí nebezpečné manipulaci a nakládání s výrobkem tak, aby ohrozil zájem na ochraně života, zdraví, bezpečnosti osob a zvířat, majetku a životního prostředí.



Obr. 1. Oblasti působnosti ÚNMZ.

Jednotlivé normativní dokumenty vydané ÚNMZ, jsou z hlediska stanovení podmínek a používání klasifikovány dle následující tabulky.

Tab. 1. Přehled vydávaných normativních dokumentů [20].

Dokument	Definice
Norma	Dokument, poskytující, pro obecné a opakované používání pravidla, směrnice, požadavky, limity nebo charakteristiky činností nebo jiných výsledků zaměřené na dosažení optimálního stupně uspořádání ve vymezených souvislostech.
Technická norma	Dokumenty, představující jakákoliv technická pravidla, směrnice nebo charakteristiky činností nebo jejich výsledků, a to ve formě mezinárodních, evropských, národních, základních, výrobkových, zkušebních, navrhovaných a dalších technických norem. Technické normy nejsou součástí právního řádu.
Česká technická norma (ČSN)	Dokument, schváleny pověřenou právnickou osobou pro opakované nebo stále použití vytvořený podle zákona č. 22/1997 a označení písmeny ČSN, jehož vydání bylo oznámeno ve Věstníku Úřadu pro ÚNMZ.
Harmonizovaná česká technická norma	Česká technická norma, která přejímá plně požadavky stanovené evropskou normou nebo harmonizačním dokumentem, které uznaly orgány Evropského společenství jako harmonizovanou evropskou normu, nebo evropskou normou, která byla jako harmonizovaná evropská norma stanovena v souladu s právem Evropských společenství společnou dohodou notifikovaných osob.
Technická normalizační informace (TNI)	Technický dokument informativního charakteru, který obsahuje technické údaje nebo technická řešení, která nejsou obsažena v platných normách (komentáře k ČSN).
Určená norma	České technické normy, další technické normy nebo technické dokumenty mezinárodních organizací, které byly ÚNMZ, určeny pro specifikaci technických požadavků na výrobky, vyplývajících z nařízení vlády nebo jiného příslušného technického předpisu. Určené normy obsahují podrobnější technické požadavky.

O technických normách lze říct, že představují dokumenty založené na souhlasu všech zainteresovaných stran se zásadními otázkami k řešení daného problému. Jsou obecně nezávazné a obsahují stanovená doporučení, nikoliv povinné příkazy. Jejich použití v určitých případech je dobrovolné, ale výhodné pro požadovanou kvalitu. Jsou vyžadovány u veřejných zakázek, kde slouží k určení referenční úrovni pověřených výrobků nebo služeb. Dále stanovují kritéria bezpečnosti a jsou nepostradatelnou podmínkou pro volný oběh zboží a služeb v rámci mezinárodního obchodu. Vyrovnávají vztah mezi jakostí a náklady, tím zvyšují ochranu spotřebitele na trhu. Jeden z požadavků je, aby použití výrobku nebo služeb byl vhodný pro daný účel na místě použití. Obsahují stanoviska na základní požadavky kvality, bezpečnosti, zaměnitelnosti, ochranu zdraví a životního prostředí.

V některých případech jsou české technické normy obecně závazné, a tím pádem jednotlivé subjekty musí dodržovat povinnosti stanoveny v českých technických normách a to na základě:

- právního předpisu (právní řád České republiky obsahuje jednotlivé předpisy, které přímo stanovují povinnost řídit se dle technických norem),
- smlouvy,
- pokynů nadřízeného pracovníka,
- stanovení správního orgánu [19].

2.2 Technické normy v oblasti integrovaných poplachových systémů

Při integraci poplachových systémů vycházíme z vydaného technického dokumentu ČSN CLC/TS 50 398. Integrování je moderním propojení poplachových a nepoplachových systémů. Poplachové aplikace jsou takové, které mají svou prioritní funkcí chránit bezpečí osob a majetku. Patří sem:

- poplachové zabezpečovací a tísňové systémy (PZTS),
- systémy přivolání pomoci (SAS),
- uzavřené televizní okruhy používaní pro bezpečností aplikace (CCTV),
- systémy kontroly vstupu (ACS),
- elektrická požární signalizace (EPS).

Požadavky na poplachové aplikace jsou obsaženy v řadě norem ČSN EN 50 13X. V rámci systému třídění norem jsou tyto řady ve většině případu přiřazeny do:

- třídy 33 - Elektrotechnika – elektrotechnické předpisy
- skupina 45 - elektrické řídící zařízení.

Příslušná čísla jsou zařazeny do struktury třídícího znaku, který obsahuje 6- místný kód a slouží nám k přiřazení norem k dané třídě a skupině. První dvě čísla v kódu představují označení příslušné třídy. Druhé dvě čísla v kódu představují označení skupiny v příslušné třídě. Systém třídících znaků pro poplachové aplikace je obsažen v rozmezí 334590 až 334597, těchto osm základních tříd odpovídá následujícím řadám norem ČSN EN 50 130 až ČSN EN 50 137.

U integrovaných poplachových systémů musí být pro každý subsystém splněn normativní požadavek aplikační normy.

Tab. 2. Přehled poplachových norem [20], upravil Macháč 2013

Základní řady norem	Název
ČSN EN 50 130 y - x	Poplachové systémy – Všeobecné požadavky
ČSN EN 50 131 y - x	Poplachové systémy – Poplachové zabezpečovací a tísňové systémy
ČSN EN 50 132 y - x	Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích
ČSN EN 50 133 y- x	Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích
ČSN EN 50 134 y - x	Poplachové systémy – Systémy přivolání pomoci
ČSN EN 50 135 y - x	Poplachové systémy - Systémy tísňové. Norma je obsažena v ČSN EN 50 131
ČSN EN 50 136 y - x	Poplachové systémy – Poplachové přenosové systémy a zařízení
ČSN EN 50 137 y - x	Poplachové systémy – Systémy kombinované a integrované v platnosti pouze ČSN CLC/TS 50 398

Nejdůležitější části z řad norem poplachových aplikací je část první, která stanovuje systémové požadavky, jejichž rozsah je třeba zvážit vzhledem příslušnému stupni zabezpečení:

- definice,
- základní principy,
- používané zkratky,
- funkční oblast systému,
- pokyny pro spolehlivý provoz,
- stupeň zabezpečení,
- druh napájeni,
- časování,
- elektrická bezpečnost,
- dokumentace a školení.

Druhá významná část z řad poplachových aplikací je část sedmá, která představuje pokyny pro aplikace, jejichž rozsah oblastí se stanovuje vzhledem k příslušnému stupni zabezpečení:

- navrhování systému,
- bezpečnostní posuzování situace v objektu,
- technický a systémový návrh,
- časový harmonogram realizace systému,

- funkční zkoušky,
- zkušební provoz [19].

Zbývající části řad poplachových aplikací představují požadavky na jednotlivé části systému (detektory, ústředny, monitory, signalizační zařízení, zobrazovací zařízení), dále stanovuje požadavky na komunikaci a vzájemné propojení jednotlivých prvků systému. Napájecí zdroje mají vlastní řadu, která stanovuje požadavky pro bezpečný provoz celého IPS.

Následně budou popsány jednotlivé oblasti technických norem v oblasti poplachových systémů, které musí být dodržené pro jednotlivé aplikace.

Technická norma v oblasti poplachových zabezpečovacích a tísňových systémů

Jednotlivé požadavky na poplachové zabezpečovací a tísňové systémy, jsou obsaženy v řadě norem **ČSN EN 50 131**. Z anglického názvu Intrusion and hold-up alarm systems (I&HAS) vyplívají dvě základní priority systému, a to:

- poplachové zabezpečovací systémy – hlavní prioritou je signalizace vniknutí do střeženého objektu,
- poplachové tísňové systémy – hlavní prioritou je signalizování různých tísňových poplachů.

Řada norem ČSN EN 50131 představuje skupinu norem vztahující se na jednotlivé oblasti systému:

- **ČSN EN 50 131- 1** - systémové požadavky,
- **ČSN EN 50 131-2-2** - detektory narušení – pasivní infračervené detektory,
- **ČSN EN 50 131-2-3** - požadavky na mikrovlnné detektory,
- **ČSN EN 50 131-2-4** - požadavky na kombinované pasivní infračervené a mikrovlnné detektory,
- **ČSN EN 50 131-2-5** - požadavky na kombinované pasivní infračervené a ultrazvukové detektory,
- **ČSN EN 50 131-2-6** - magnetické kontakty – detektory otevření,
- **ČSN EN 50 131-2-7-1** - detektory narušení – detektory rozbíjení skla (akustické),
- **ČSN EN 50 131-2-7-2** - detektory narušení – detektory rozbíjení skla (pasivní),
- **ČSN EN 50 131-2-7-3** - detektory narušení – detektory rozbíjení skla (aktivní),
- **ČSN EN 50 131-3** - ústředny,

- **ČSN EN 50 131-4** - výstražná zařízení,
- **ČSN EN 50 131-5** - požadavky na zařízení využívající bezdrátové propojení,
- **ČSN EN 50 131-6** - napájecí zdroje,
- **ČSN EN 50 131-7** - pokyny pro aplikace,
- **ČSN EN 50 131-8** - zamlžovací bezpečnostní zařízení/systémy [19].

Účel normy ČSN EN 50 131-1 je zpřesnit a zefektivnit práci instalačních pracovníků, pojišťovnám, investorům, uživatelům a státním orgánům. Stanovuje přesné specifikace na technickou ochranu zabezpečovaného objektu. Tyto specifika jsou obsaženy v **systémových požadavcích**, které musí být konkretizovány na místě nasazení prvků systémů.

Norma ČSN EN 50131-7 představuje **aplikační pokyny** pro navrhování, montáž, provoz a údržbu poplachových zabezpečovací a tísňových systémů. Při projektování PZTS stupně zabezpečení 3 a vyšší je kladena podmínka na odbornou způsobilost, kde projektant musí splňovat příslušnou autorizaci podle zákona č.360/1992Sb., o výkonu povolání autorizovaných inženýrů a techniků činných ve výstavbě. V oblasti poplachových systémů se jedná o autorizaci v oboru: technika prostředí staveb – specializace elektrotechnická zařízení [21].

Jednotlivé **požadavky na integraci PZTS**, stanovené příslušnou aplikační normou ČSN EN 50 131-1,7:

- obecné požadavky, týkající se vzájemné **kompatibility výrobků**, konzultace na úrovni výrobce, dovozce a zkušebny,
- dělí kabelové propojení na **specifické** (v rámci jedné aplikace) a **nespecifické** (mezi více aplikacemi),
- požadavky na **zpracování** signálů,
- požadavky na **signalizaci** stavu systému.

Technická norma v oblasti CCTV sledovací systémy pro použití v bezpečnostních aplikacích

Touto problematikou se zabývá řada norem **ČSN EN 50 132** Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích.

Norma představuje dílčí skupiny norem vztahující se na:

- **ČSN EN 50 132-1** - systémové požadavky,
- **ČSN EN 50 132-5-1** - video přenosy – obecné provozní požadavky,
- **ČSN EN 50 132-5-2** - IP video přenosové protokoly,
- **ČSN EN 50 132-5-5** - přenos videosignálu,
- **ČSN EN 50 132-7** - pokyny pro aplikaci [19].

Všeobecně řečeno, kamerové systémy díky moderní technologii prokazují kvalitní zpracování digitálního obrazu, a tím spolehlivé vyhodnocení snímané scény. Proto jejich využití v poplachových aplikacích je poslední dobou moderní a nově zavádějící.

Další oblasti, které jsou zpracovány na vydání v rámci řady této normy:

- černobíle kamery,
- barevné kamery,
- objektivy,
- příslušenství,
- místní a hlavní řídící jednotka,
- monitory,
- záznamová zařízení,
- zařízení pro okamžitý výtisk obrazu,
- videodetektor pohybu.

ČSN EN 50132-1- **Systémové požadavky**, kde norma se vztahuje na systémy CCTV užívané pro monitorování soukromých a veřejných prostor. Nově se definují čtyři stupně zabezpečení a čtyři třídy vlivu prostředí. Systémové požadavky jsou vhodné pro výrobce, systémové integrátory, montážní firmy, konzultanty, majitele, uživatele, pojišťovny a společnosti zajišťující prosazování práva v dosažení kompletní a přesné specifikace sledovacího systému. Norma nespecifikuje žádné typy technologií, ani požadavky na kvalitu obrazu pro konkrétní úlohy sledování v místě nasazení [19].

ČSN EN 50 132-7 – **Pokyny pro aplikaci**, následující část normy stanovuje doporučení pro výběr, plánování a instalaci systémů uzavřených televizních okruhů, které zahrnují kamery s monitory anebo s videorekordéry, řídicí a ostatní pomocná zařízení nutná pro použití v bezpečnostních aplikacích.

Cílem normy je:

- poskytovat pracovní rámec umožňující zákazníkům, instalačním firmám a uživatelům stanovit jejich požadavky,
- pomoci projektantům a uživatelům při výběru optimální varianty zařízení,
- poskytnout prostředky k objektivnímu hodnocení vlastností instalovaného kamerového systému [22].

Jednotlivé oblasti, které stanovují určité **požadavky na integraci CCTV**, jsou obsaženy v aplikační normě ČSN EN 50 132-1:

- obecné požadavky na **formát dat**
- **možnosti integrace** s dalším systémem:
  - PZTS,
  - ACS,
  - bankomaty,
  - dohledové poplachové a přijímací centrum,
  - rozpoznání SPZ,
  - inteligentní dům,
  - systém řízení budovy.

Technická norma v oblasti systémů kontroly vstupu pro použití v bezpečnostních aplikacích

Normativní požadavky na systémy kontroly vstupů pro využití v bezpečnostních aplikacích jsou obsaženy v řadě normy **ČSN EN 50 133**. Nasazení systému kontroly vstupu, zavádíme do organizace i režimová opatření, které musí být stanovena tak, aby bylo v souladu se softwarovou částí přístupového systému.

Norma ČSN EN 50 133 představuje vydané dílčí skupiny normy:

- **ČSN EN 50 133-1** - systémové požadavky,
- **ČSN EN 50 132-2-1** - všeobecné požadavky na komponenty,
- **ČSN EN 50 132-7** - pokyny pro aplikace.

ČSN EN 50 133-1 **Systémové požadavky** - vztahující se na jednotlivé aplikace od všeobecných požadavků na funkčnost systému kontroly vstupů a všeobecné požadavky na komponenty z hlediska prostředí instalace [19].

ČSN EN 50 133-7 **Pokyny pro aplikace** – norma uvádí pokyny k použití automatizovaných systémů kontroly vstupů a komponentů uvnitř a vně budov na základě obsahu norem EN 50 133. Vztahují se na návrh systému, instalaci, předávání, provoz a údržbu systémů kontroly vstupů [23].

Pokyny jsou určeny pro všechny systémy kontroly vstupů použité v bezpečnostních aplikacích. Od ovládání jednoho přístupového místa až po složité systémy s mnohanásobnými přístupovými místy.

Systém kontroly vstupů může být propojen s různými druhy poplachových systémů (PZTS, CCTV). **Požadavky na integraci** jsou stanoveny v aplikační normě ČSN EN 50 133 - 1, která stanovuje jednotlivé postupy v **oblasti komunikace** s ostatními systémy a zavádí se požadavky na:

- výstupy systému (galvanicky, binárně oddělené spínače,
- stavy výstupů na základě časové reakce,
- logické informace,
- programovaní,
- komunikační linky.

Technická norma v oblasti systémů přivolání pomoci

Norma specifikuje doporučení, které jsou uvedeny ve třídě **ČSN EN 50 134**. Zabývá se systémy přivolání pomoci, které jsou nezbytná pro každou efektivní záchranu lidského života.

Norma popisuje požadavky na:

- aktivování poplachu,
- identifikaci,
- přenos signálu,
- přijetí poplachu a potvrzení,
- záznam a obousměrnou hlasovou komunikaci,
- třídu prostředí ovlivňující návrh systému.

Norma představuje vydané dílčí řady ČSN EN 50 134 vztahující se na:

- **ČSN EN 50 134-1** - systémové požadavky,
- **ČSN EN 50 134-2** - aktivační zařízení,

- **ČSN EN 50 134-3** - místní jednotka a kontrolér,
- **ČSN EN 50 134-5** - propojení a komunikace,
- **ČSN CLC/TS 50 134-7** - pokyny pro aplikace [19].

Norma udává možná doporučení na propojení osob žijících doma s určitou zdravotní zátěží a dohledovým, poplachovým přijímacím centrem (DPPC). Systému využívá drátových přenosů, např. pronajaté linky, pevné drátové propojení, vedení optickými vlákny nebo bezdrátových, např. rádiovou síť, buňkový systém, infračervený přenos.

Dále upravuje doporučení na zkoušky technologii, tvořící část systému přivolání pomoci. Důležitá součást je DPPC, které přijímají spuštěný poplachový signál z ručně nebo automaticky spouštěného aktivačního [24].

Technické normy v oblasti poplachových přenosových systémů a zařízení

Norma specifikuje doporučení, které jsou uvedeny ve třídě **ČSN EN 50 136**. Zabývá se propojením jednoho nebo více systémů, kde požadavky jsou kladeny na zařízení a přenosové sítě.

Norma ČSN EN 50 136 představuje vydané dílčí skupiny normy dělící se na:

- **ČSN EN 50 136-1** - obecné požadavky na poplachové přenosové systémy,
- **ČSN EN 50 136-1-1** - všeobecné požadavky na poplachové přenosové systémy,
- **ČSN EN 50 136-1-2** - požadavky na systémy využívající vyhrazené poplachové přenosové cesty,
- **ČSN EN 50 136-1-3** - požadavky na systémy s digitálními komunikátory využívajícími veřejnou komutovanou telefonní síť,
- **ČSN EN 50 136-1-4** - požadavky na systémy s hlasovými komunikátory využívajícími veřejnou komutovanou telefonní síť,
- **ČSN EN 50 136-1-5** - požadavky na paketově přepínanou síť PSN,
- **ČSN EN 50 136-2-1** - všeobecné požadavky na poplachová přenosová zařízení,
- **ČSN EN 50 136-2-2** - požadavky na zařízení v systémech využívajících vyhrazené poplachové přenosové cesty,
- **ČSN EN 50 136-2-3** - požadavky na zařízení v systémech s digitálními komunikátory využívajícími veřejnou komutovanou telefonní síť,

- **ČSN EN 50 136-2-4** - požadavky na zařízení v systémech s hlasovými komunikátory využívajícími veřejnou komutovanou telefonní síť,
- **ČSN EN 50 136-4** - indikační a ovládací zařízení používaná v DPPC,
- **ČSN EN 50 136-7** - pokyny pro aplikace.

ČSN EN 50 136-**7 Pokyny pro aplikace** – Tato část normy upravuje doporučení na aplikaci v oblasti poplachových a přenosových zařízení a systémů. Norma představuje vhodné pokyny pro poplachové přenosové systémy, indikační a ovládací zařízení. Pokyny se týkají konkrétních aplikací, které napomáhají především montážním firmám zabývající se poplachovými přenosovými systémy [19].

ČSN EN 50 136-1 **Obecné požadavky na poplachové přenosové systémy -** norma stanovuje požadavky v oblastech výkonnosti, spolehlivosti a bezpečnosti poplachových přenosových systémů. Obsahuje obecné požadavky na propojení dané signalizace mezi poplachovým systémem ve střežených objektech a ohlašovacím zařízením v DPPC. Tato norma se aplikuje pro všechny přenosové systémy s obsahem zprávy typů; vloupání, řízení přístupu, požár, přivolání pomoci, sabotáž, hlášení poruch a stavová hlášení [25].

2.2.1 ČSN CLC/TS 50 398

V následující podkapitole je čerpáno z české verze technické specifikace CLC/TS 50398:2009. Vydání překladu provedl ÚNMZ, který oficiálně vydal aktuální verzi v říjnu 2009.

Norma představuje všeobecné požadavky a typy struktur kombinovaných a integrovaných poplachových systémů. Norma doporučuje stanoviska k integraci jedné nebo více aplikací do jednoho integrovaného systému.

Tento normativní dokument poskytuje další informace týkající se:

- prvotního návrhu systému,
- plánování, instalace,
- předávání,
- provozu,
- údržby kombinovaného a integrovaného systému.

V normě jsou také specifikovány požadavky na poplachové systémy, které jsou kombinovány nebo integrovány s nepoplachovými systémy. Obsahuje požadavky týkající se pravidel integrace a respektování jednotlivých aplikačních norem jednotlivých systémů [26].

Struktura ČSN CLC/TS 50 398

1. Rozsah platnosti
2. Citované normativní dokumenty
3. Definice
4. Všeobecný popis a základní principy
5. Systémové požadavky a stanovení kompatibility
6. Dokumentace a školení

Příloha A (informativní) Směrnice pro použití a montáž, spolehlivost

Rozsah platnosti

- Požadavky na poplachové systémy integrované nebo kombinované s ostatními nepoplachovými systémy.
- Požadavky k integraci, s cílem doplnit jednotlivé aplikační normy poplachových systémů a pomoc s objasněním tam, kde dochází ke konfliktu.
- Nezahrnuje poplachové přenosové systémy.

Definice

Přesné pojmenování a vymezení pojmů je stěžejní při pochopení problematiky integrovaných nebo kombinovaných systémů. Pro účel této normy jsou přesně stanoveny následující definice:

doplňkové zařízení – zařízení, které není v žádné aplikaci integrovaného poplachového systému vyžadovanou příslušnou normou,

poplach – upozornění na aktuální nebezpečí ohrožující život, majetek nebo životní prostředí,

poplachová aplikace – výhradně určené aplikace na ochranu života majetku nebo životního prostředí:

- poplachový zabezpečovací a tísňový systém,
- systém přivolání pomoci,
- poplachový systém výtahů,

- poplachový systém vlivu prostředí,
- kamerové systémy CCTV,
- systém kontroly vstupu,
- elektrická požární signalizace,

poplachové přijímací centrum – trvale obsluhované středisko, které přijímá informace týkající jednoho nebo více poplachových systémů,

poplachový systém – elektrické zařízení reagující na manuální podnět nebo na automatickou detekci aktuálního nebezpečí,

poplachový přenosový systém (ATS) – síť tvořící zařízení používané pro přenos informací mezi poplachovými systémy a poplachovými přijímacími centry,

aplikace – zařízení využívané pro specifické účely, například detekce a výstraha při vzniku požáru, ovládání klimatizace, osvětlení, atd.,

aplikační norma – norma udávající požadavky na instalaci a provoz příslušné aplikace,

ústřední ovládací zařízení (CCF) – zařízení výhradě používané při řízení (ovládání) systému a/nebo signalizaci ve struktuře integrovaných poplachových systémů, připojené k jednomu nebo více jednoúčelových systémům, obvykle obsluhovaný personálem,

společné zařízení – zařízení, které je sdíleno jednou nebo vice aplikacemi,

zařízení – hardwarové nebo softwarové části zařízení, které umožňují systému plnit jednu nebo více funkcí,

integrovaný poplachový systém – systém obsahující jedno nebo více společných zařízení, alespoň jedním v systému je poplachová aplikace,

- poplachový přenosový systém se nepovažuje za součást IPS,
- jednoúčelové systémy připojené pouze přes jednosměrný výstup zařízení bez jakéhokoli přenosu dat (relé),

integrita – schopnost aplikace plnit stanovené funkce, pro něž je použita, včetně odolnosti vůči vlivům, které by mohli ovlivnit její správnou funkci,

nepoplachová systémy – systémy používané pro ovládání (řízení) a jejichž primární funkcí není ochrana života, majetku nebo prostředí (osvětlení, ventilace, správa budovy, energetické systémy, výtahy),

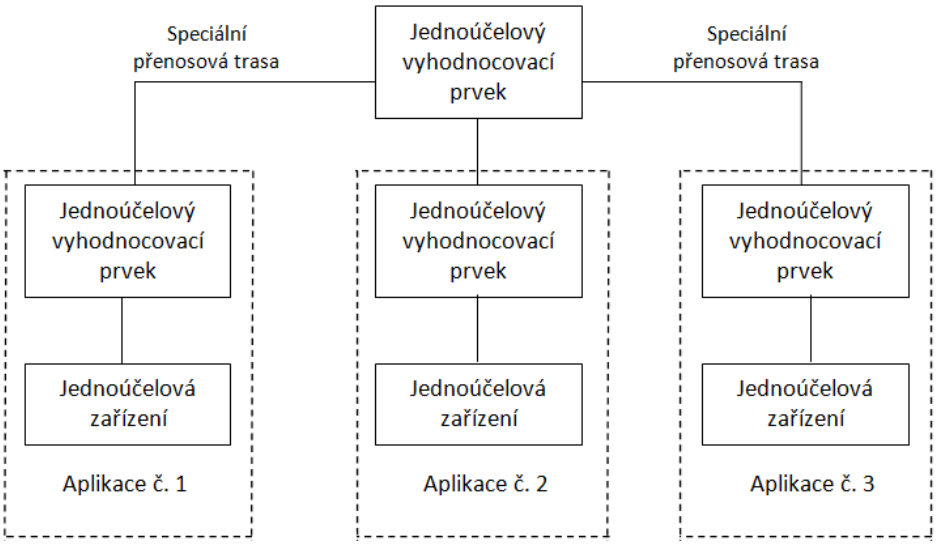
normou vyžadované zařízení – zařízení, které je nezbytné pro správné splnění požadavků normy příslušné aplikace [26].

Všeobecný popis a základní principy

Tři základní specifikované konfigurace/typy integrovaných poplachových systémů:

- **Typ 1** je použitelný pro kombinaci a integraci jednoúčelových poplachových systémů a jednoúčelových nepoplachových systémů.

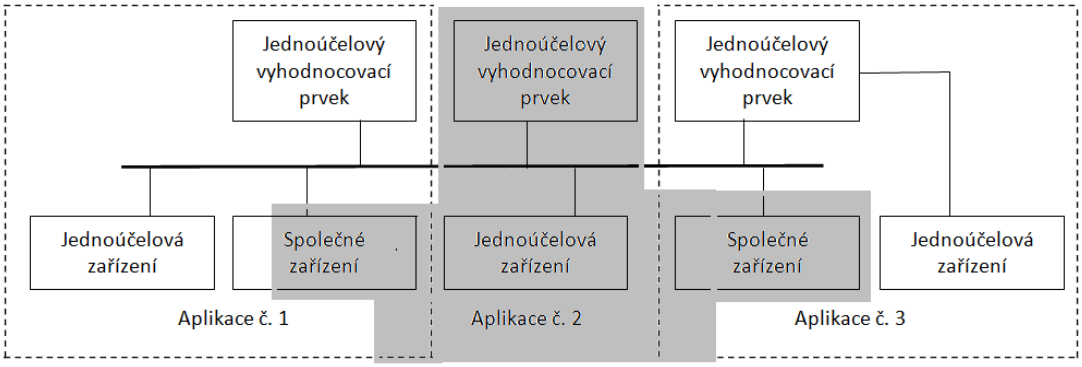
  Jednoúčelové systémy jsou připojeny ke společnému doplňkovému zařízení, například společná doplňková trasa. Vyžadované zařízení aplikační poplachovou normou nesmí být v žádném provozním stavu negativně ovlivněno dalším jednoúčelovým systémem nebo doplňkovým zařízením. Převážně společné doplňkové zařízení, které nejsou požadovány příslušnou aplikační normou, musí splňovat požadavky technické specifikace CLC/TS 50398.



Obr. 2. Konfigurace typu 1, (CCF - třídy 1) [26].

- **Typ 2A** je použitelný pro kombinaci a integraci poplachových systémů a nepoplachových systémů, využívající výhradně společné přenosové trasy, společná zařízení a společné vybavení. Porucha v jakékoliv aplikaci **nemá žádný negativní účinek** na všechny další poplachovou aplikaci. Získání tohoto stavu je potřeba znásobení (nadbytečnost).

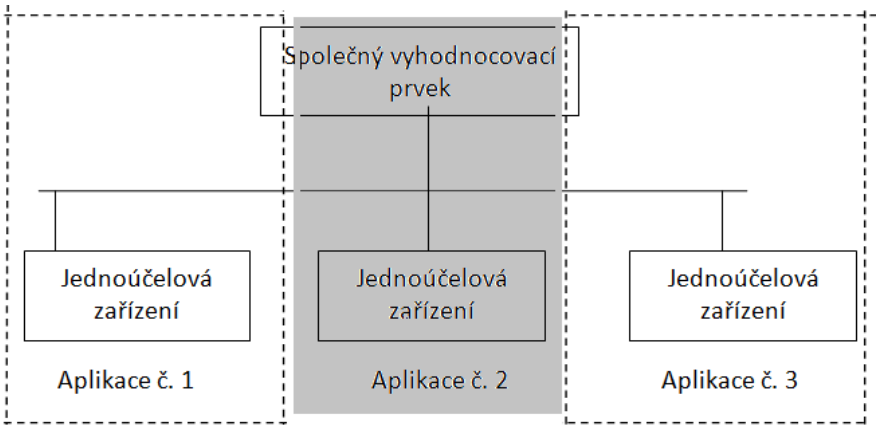
  V tomto typu konfigurace nesmí být integrita všech normou vyžadovaných poplachových zařízení nepříznivě ovlivněna žádnou poruchou v ostatních aplikací.



Obr. 3. Konfigurace typu 2A [26].

- **Typ 2B** je použitelný pro kombinaci a integraci poplachových systémů a nepoplachových systémů využívající výhradně společné přenosové trasy, společná zařízení a společné vybavení. Porucha v jedné aplikaci **může mít negativní účinek** na ostatní poplachovou aplikaci.

  V tomto typu konfigurace může být integrita všech normou vyžadovaných poplachových zařízení nepříznivě ovlivněna jedinou poruchou v ostatních aplikacích.



Obr. 4. Konfigurace typu 2B [26].

Systémové požadavky a stanovení kompatibility

Integrovaný poplachový systém musí být projektován takovým rozmyslem, aby nebyla žádná aplikace jak v normálním tak i poplachovém stavu nepříznivě ovlivněna žádnou jinou aplikací. Této komplikaci můžeme předcházet správnou organizací pohybu informací v systému.

Využívání takzvaných **povelových signálů** povede ke správné organizaci informací, vhodné využití převážně u správy velkých objektů skládající se i z většího počtu budov. Při špatné konfiguraci zařízení může také snížit bezpečnost a zabezpečení systémů. Přenos informací probíhá mezi jednotlivými aplikacemi nebo z ústředního ovládacího zařízení (CCF) do dalších částí systému.

Stanovení **přístupové úrovně** u každé aplikace integrovaného poplachového systému zamezí nepovolené manipulaci a konfiguraci zařízení neoprávněnou osobou. Přístupové úrovně jsou stanoveny v souladu příslušnou aplikační normou [26].

Společné ovládací zařízení je sdílené více než jednou aplikací, jeho ovládání musí být pro uživatele jasné a jednoznačné. Na uživatelském rozhraní musí být zřetelně indikována aplikace, která je tímto rozhraním ovládaná.

Společné signalizační zařízení můžeme být normou vyžadované, nebo chápáno jako doplňkové zařízení. U normou vyžadovaného zařízení musí splňovat nejpřísnější požadavky definované v normách. U doplňkového zařízení, musí být spolehlivost signalizace události úměrná jejímu významu ve smyslu důležitosti informace na následná opatření.

Efektivitu signalizaci informací zvýšíme přiřazením jednotlivým událostem barvy. Pro kritické informace potřebné pro rychlou reakci musí být použité barvy, které jsou vybrané dle daného osvětlení zařízení. Některé příslušné normy přesně definují jednotlivé barvy, v případě rozporu mezi normami musí signalizace vycházet s požadavků normy EN 60073.

Priority informací musí být posouzeny dle požadavků. Priority signalizování informací musí být jasně a jednoznačné stanoveny. Z obecného hlediska by měly vycházet z následujících priorit:

- priorita 1 – poplachové signály (ochrana života, požár, napadení),
- priorita 2 – poplachové signály (ochrana majetku, nedovolené vniknutí),
- priorita 3 – poplachové signály z ostatních poplachových aplikací,
- priorita 4 – poruchové signály (ochrana života a majetku),
- priority 5 – poruchové signály z ostatních poplachových aplikací,
- priority 6 – informace z nepoplachových aplikací.

Všeobecné požadavky na priority signalizace:

- možnost zobrazení doplňkových informací na zadaný příkaz,
- jakákoliv činnost aplikace nesmí omezit indikaci poplachu,
- signalizovat stav, kdy existují poplachy z více aplikací,
- nezobrazovat opakovaný poplachový signál,
- signalizace stavu, kdy již není možné zobrazit všechny poplachy [26].

Integrita normou vyžadovaných prvků, je chápána jako společný monitoring s možností detekovat a signalizovat selhání monitorovací sekvence jednotlivých aplikací. Společný procesní prvek nese v sobě riziko selhání správy systému a tím pádem omezení řízení, proto je potřeba zálohovat příslušná dat. Použitý software společných vyhodnocovacích prvků je doporučené oddělit pro každou aplikaci samostatně a popsat možné účinky a ovlivnění softwarových částí systému.

Připojení k poplachovému přenosovému systému (ATS) - síť tvořící zařízení používané pro přenos informací mezi poplachovými systémy a poplachovými přijímacími centry. Je li ATS využíván více aplikacemi je možné k němu připojit pouze ty části integrovaného poplachového systému splňující aplikační normy. Nastavením priorit ATS, lze využít i pro přenos doplňkových informací.

Spolehlivé **propojení** zařízení spočívá v dodržování příslušných aplikačních norem. Zařízení, které nejsou uvedené v žádných normách, musí splňovat následující požadavky v provozu:

- akceptovat jen povely, které jsou obsaženy v aplikačních normách,
- neidentifikovatelné signály nemají nepříznivý vliv,
- všechna použita zařízení musí obsahovat funkci signalizaci sabotáže a monitoringu zařízení.

Napájecí zdroje jsou určeny v IPS jako speciální a/nebo společné zařízení, které nesmí ohrozit požadavky napájecích zdrojů dle použité aplikační normy.

Požadavky týkající se **časování** v IPS spadají na přenos informací mezi normou vyžadovaného zařízení a doplňkového zařízení. Přenos musí být realizován tak, aby byl schopný přijaté informace zpracovat v 150% době specifikované v příslušné normě. Pro každou aplikaci musí být splněny požadavky na časování, které jsou obsaženy ve všech příslušných normách.

Prověření provozuschopnosti u každé aplikace musí vycházet ze svých stanovisek určené v příslušné normě. Provozuschopnost u IPS by měla být stanovena tak, aby bylo zaručeno spolehlivé fungování, v souladu s předem stanoveným plánem příčina-účinek. Plán může být specifikován výrobcem, montážní firmou, pojistitelem, zákazníkem nebo regulačním úřadem. Oblasti provozuschopnosti:

- zkouška v normálním, poplachovém i poruchovém stavu,
- postupy ovládání IPS a jednotlivých částí,
- dokumentace provedené zkoušky [26].

Centrální ovládací zařízení (CCF)

zařízení výhradě používané při řízení (ovládání) systému a/nebo signalizaci v IPS, připojené k jednomu nebo více jednoúčelových systémům, obvykle obsluhovaný personálem. Lze jej klasifikovat do dvou následujících tříd.

- **Třída 1** – použití jen k zobrazování informací v prostorách s provozní obsluhou + normou vyžadované signalizační zařízení (signalizační panel, ústředny) musí být ve stejných prostorech. Při poruše CCF bude signalizace poplachu zaznamenána obsluhou.
- **Třída 2 –** použití jen k zobrazování informací v prostorách s provozní obsluhou a to jako jediný signalizační prvek. Zda li CCF dokáže ji nastavování stavu střežení/klid, zapnutí/vypnutí, ukládání parametrů musí být toto zařízení plně v souladu s aplikačními normami.

Všeobecné požadavky na CCF:

- identifikovat příslušnou třídu použití CCF,
- umístit do příslušného prostředí,
- nevyužívat mimo IPS.

Požadavky na CCF II:

- provoz monitorován v místě jeho použití,
- porucha CCF je signalizovaná akusticky i opticky,
- monitoring napájení,
- signalizace výpadku jednotlivé monitorovací sekvence,
- plán postupů při poruše CCF,
- monitorovat komunikace s aplikacemi dle požadavku určených norem,

- záložní zdroj na dobu minimální ke splnění nezbytných postupů [26].

Dokumentace a školení musí být zpracována pro IPS stručně, úplně a jednoznačně. Uvedené informace musí být vhodné pro montáž, oživení systému, vlastní provoz a údržbu systému. Musí být stanoven typ konfigurace systému. Je li použito CCF musí být uvedena třída použití a stanoveny specifika prostředí. Splnění požadavků aplikačních norem na dokumentaci. Zpracování školících manuálů pro obsluhu IPS, která by měla být v pravidelných intervalech přezkoušena [26].

2.3 Vlivy prostředí

Funkčnost integrovaného poplachového sytému neovlivňují jen použité zařízení, ale i vlivy vnějšího prostředí. Existují různé druhy působení vnějších vlivů, které pomocí svých fyzikálních jevů dovedou ovlivnit funkčnost určitého prvku nebo i celého systému.

Zkoušky vlivů prostředí pro všechny poplachové aplikace jsou popsány v normě ČSN 50130-5. V této normě jsou uvedeny různé sady zkoušek, k určení schopnosti zařízení vykonávat svou funkci, pro kterou byl vyroben. Zkoušky jsou rozděleny do dvou skupin:

- **provozní zkoušky** – podmínky odpovídající provozním podmínkám,
- **odolnostní zkoušky** – přísnější podmínky než normální provoz.

Důsledkem působení vlivů prostředí byly stanoveny čtyři třídy prostředí:

I. **vnitřní –** prostředí bytů, kanceláře,
II. **vnitřní všeobecné –** prostředí obchodů, restaurace, výrobní a montážní haly,
III. **venkovní –** prostředí chráněné proti přímému dešti, slunci, nebo vnitřní prostory s extrémními podmínkami (garáže, půdy, stodoly, překladiště),
IV. **venkovní všeobecné** – prostředí vystavené přímému působení venkovních vlivů[27].

Ke třídám III a IV je vydána speciální příloha, upravující požadavky na zařízení, které budou použita v severních částech Evropy, kde venkovní podmínky jsou extrémnější než v jiných částech kontinentu.

V následující tabulce jsou uvedené oblasti jednotlivých zkoušek a příslušné vlivy prostředí.

Tab. 3. Vlivy prostředí a případné zkoušky [26], upravil Macháč 2013

Suché teplo	Provozní vysoké teploty okolí a odolnost vlivů stárnutí
Chlad	Provozní nízké teploty okolí
Změna teploty	Provozní rychlé změny teploty okolí
Vlhké teplo	Vysoká relativní vlhkost vzduchu
Vniknutí vody	Chránění proti vniknutí vody
Oxid siřičitý	Odolnost vlivu SO_2 jako znečišťovatele ovzduší
Solná mlha	Ochrana proti korozi chemickým vlivům
Úder	Mechanická odolnost úderů na povrchu zařízení
Volný pád	Odolnost při neopatrné manipulaci
Vibrace	Odolnost vůči provozním vibracím
Sluneční záření	Vystavení tepelných vlivů a degradace slunečního záření
Prachotěsnost	Odpovídající ochrana vniku jemného prachu
Elektromagnetická kompatibilita	Specifikování požadavků na EMC stanovené v ČSN EN 50130-4

Elektromagnetická kompatibilita (EMC)

Oblast vzájemného rušení je u integrovaných poplachových systémů velmi zrádná, a proto musíme brát v úvahu provádění zkoušek u používaných zařízení. Stanovení požadavků na odolnost poplachových aplikací je uvedeno v normě **ČSN EN 50130-4**. Kde je uvedeno, že zkoušky se musí provádět:

- postupně, jak stanovuje norma,
- zařízení musí splňovat kritéria požadavků pro každou zkoušku,
- pokud je více zkoušek na zařízení provádí se volitelně,
- pomocné funkční zkoušky,
- chybu nelze přiřadit zkoušce.

V elektromagnetické kompatibilitě se provádí zkoušky v oblasti:

- změny oblasti napájecího napětí,
- poklesů a krátkodobého přerušení síťového napájecího napětí,

- elektrostatického výboje,
- vyzařování elektromagnetického pole,
- rušení indikovaného elektromagnetického pole,
- rychlých přechodových jevů,
- pomalých rázových napěťových impulsů[28].

Dílčí závěr

Při instalaci, revizi, údržbě a dalších úkonech u integrovaného systému se musí vycházet z technických požadavků, které jsou obsaženy v příslušných normách aplikace. Dodržování podmínek, které jsou uvedeny v příslušných aplikačních normách, vede ke zvýšení efektivity, komfortu a bezpečnosti celého integrovaného systému.

Technické požadavky týkající se nepoplachových aplikací jsou obsaženy v hodně širokém spektru použití, jelikož dnešní doba se snaží vše miniaturizovat a integrovat.

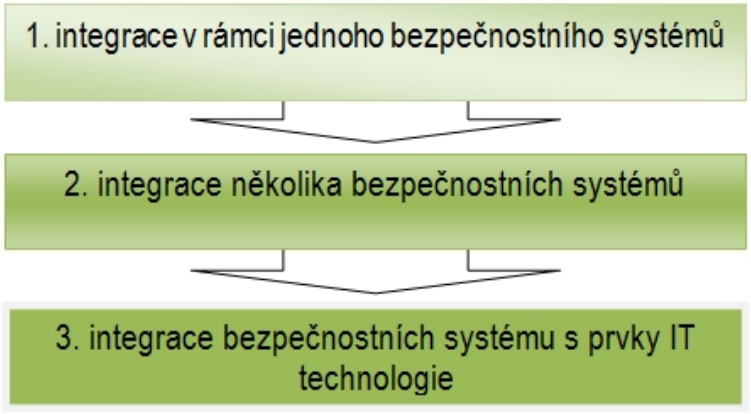
Přímo integrace systému s využitím prvků informační technologie má stanovené podmínky, jen částečně v normě ČSN CLC/TS 50 398. U integrace poplachových systémů musí být použity příslušné normy pro každou aplikaci systému.

3 INTEGROVANÉ SYSTÉMY

Všeobecně integrované systémy představují propojení poplachových a nepoplachových aplikací. U každého integrovaného systému je propojení jednotlivých systémů na určité úrovni, která dokáže reagovat a akceptovat informace z propojených zařízení.

Hlavním cílem v této kapitole je objasnit jednotlivé úrovně, funkce a třídy propojení poplachových a nepoplachových aplikací do jednoho integrovaného systému.

Jednotlivé stupně integrace lze rozdělit do tří skupin, které určují vzájemné propojení systémů.



Obr. 5. Stupně integovaných systémů [8].

První stupeň integrovaného propojení v rámci **jedné aplikace** vychází například ze systému kontroly přístupu, kde jsou čtečky karet, ovládací klávesnice, monitorovací a identifikační prvky osob integrovány do jednoho systému, který obsahuje i správu karet.

Druhý stupeň integrace si lze představit jako propojení **dvou a více aplikací**, například propojením kontroly vstupů se zabezpečovací signalizací, kamerovým systémem, elektrickou požární signalizací, tísňovýma tlačítky a perimetrickou ochranou objektu do jednotného uživatelského rozhraní.

Třetí stupeň integrace využívá **prvky informační technologie**. Tento stupeň je zatím nejvyšší možnost propojení jednotlivých systémů, vychází z propojení na místní vybudované síti.

Postup realizace integrovaných poplachový systémů ovlivňují také **obchodní aspekty.**

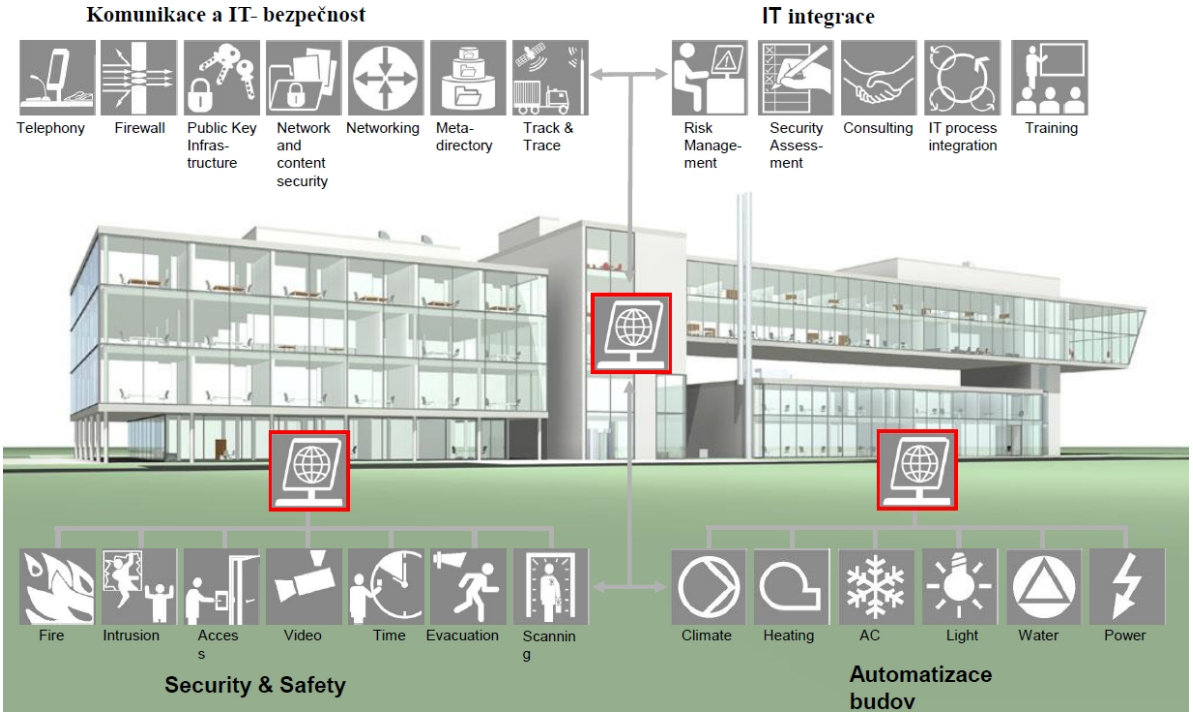
Dodavatelský řetězec a vztahy průběhu realizace IPS představují:

- dodavatele stavebních částí,
- výrobci hardware,
- výrobci software,
- dodavatelé infrastruktury – IT, energie,
- instalační firmy,
- projektant,
- systémový integrátor,
- uživatel/provozovatel,
- majitel – investor,
- inspekce – státní orgány
- dodavatelé služeb,
- nájemce/nájemníci,
- návštěvníci[29].

3.1 Konfigurační možnosti systémů

Určení jednotlivých konfiguračních topologii integrovaných systémů vychází ze vzájemného propojení jednotlivých zařízení, které mezi sebou přenášejí a reagují na různé druhy informací vyvolávající určitou reakci. V současné době představuje trh velké možnosti různého propojení jednotlivých systémů, většinou jsou systémy děleny dle dislokace do tří hlavních skupin.

- **Komerční systémy** – požadavky se vztahují na:
    - prevenci vniknutí nepovolených osob do objektu,
    - prevenci před nežádoucí činností osob povolaných (zaměstnanci),
    - **bezpečnostní přínos** – přehlednost celkové situace a automatizovaného provázání systémů při řešení havarijních a evakuačních postupů.
    - **ekonomický přínos** – úspora energie při vytápění, klimatizaci a osvětlení, dále úspora na mzdách a správě objektu.
    - **technický přínos** – zjednodušení činnosti obsluhy, školení pracovníků, funkční propojení systémů, jednotný systém pro všechny.



Obr. 6. Příklad konfigurační možnosti - komerční objekt [30].

- **Rezidenční systémy** – požadavky se vztahují na:
  - **velké množství** ovládané A/V techniky, světel a dalších zařízení,
  - každé zařízení, které **vlastní ovladač**/klávesnici/panel,
  - vzdálenost ovládaných zařízení pro **komfort** uživatele,
  - složité ovládání,
  - dálkové ovládání celého systému z různých míst domu,
  - ovládaná zařízení s žádnou/malou zpětnou vazbou.

S požadavků kladené uživatelem, převažují tyto tři základní složky ovlivňující návrh:

- **jednoduché ovládání,**
- **pouze podstatné ovládací funkce,**
- **finančně realizovatelné** [8].

Obr. 7. Příklad rezidenčího systému [31].

- **Městské a obecní systémy** – požadavky se vztahují na:
  - činnost operátora, příjem hovorů, alokace zdrojů,
  - geografické informace, vizualizace daného prostředí na mapě,
  - ovládání a zobrazování videosignálu z kamerového systému,
  - varovné systémy, zobrazení stavů koncových zařízení,
  - GPS, sledování objektu, vzdálenosti a dojezdové časy,
  - PPC (PZTS, EPS), poloha střežených objektů, místění prvků ochrany,
  - reakce systému na následné události, odeslání zpráv události,
  - statistiky potřebné k rozhodování [8].

Obr. 8. Přijímací centrum městských systémů [30].

3.1.1 Struktura

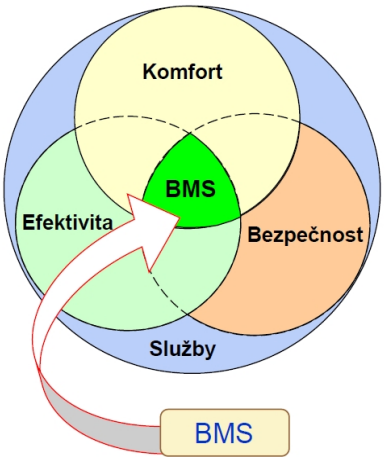
Integrované poplachové systémy jsou ideálním řešením v oborech, na které jsou kladené vysoké požadavky na přenos a zpracování informace. Propojení poplachového zabezpečovacího systému, přístupového a kamerového systému, řízení výtahu, ovládání osvětlení, ozvučení, klimatizace a dalších technologických i administrativních procesů na úrovni daného objektu s využitím prvků informační technologie přináší například tyto výhody:

- řízení přístupu osob do jednotlivých částí objektu + uživatelská databáze,
- více informací o bezpečnostní situaci,
- vazba na mzdový systém firmy,
- kontrola odběru a úspora energie,
- centralizovaná obsluha,
- úspora na kabeláži,
- univerzálnost a flexibilita,
- ovládací a vizualizační SW.

Integrované poplachové systémy, které ve své struktuře používají **prvky informační technologie,** najdou převážně uplatnění u::

- **bezpečnostních složek,**
- **kritické infrastruktury,**
- **velkých společností,**
- **inteligentních budov** [32].

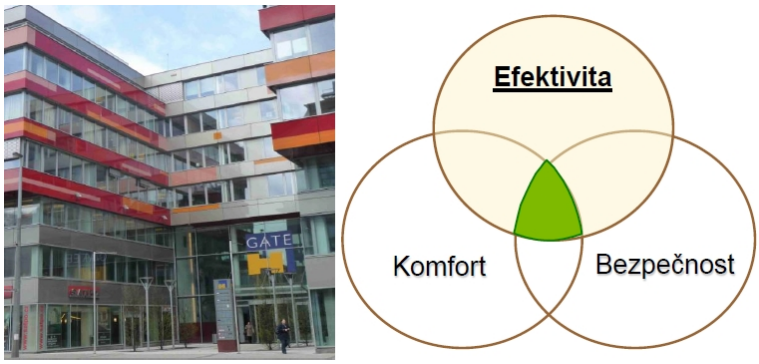
Struktura každého integrovaného poplachového systému vychází hlavně z požadavků klienta, které se převážně týkají **bezpečnosti, efektivity, komfortu a služby** celého projektu integrovaného poplachového systému. Jednotlivé požadavky lze integrovat do **role řídicího systému budov (building management system - BMS)**, ze kterých se vychází už při prvotním zadávání zakázky.



Obr. 9. Prvky BMS [32].

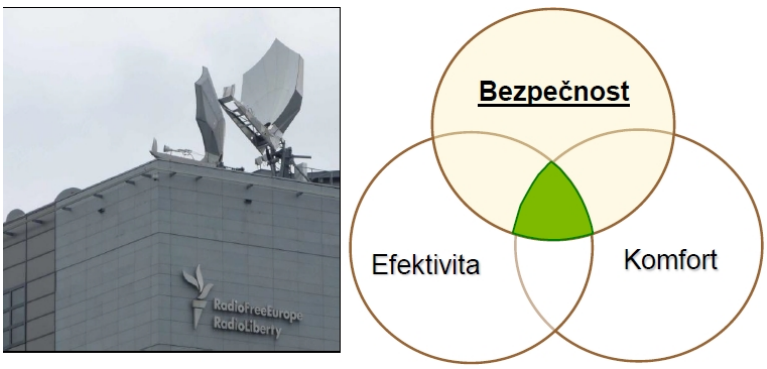
Integrací rozumíme **provázání funkce jednotlivých systémů.** Díky vzájemnému propojení docílíme zpracování informací všech systémů v jednotném prostředí a komfortu. Možnost přímého využití dat jednoho ze systémů v ostatních provázaných systémech. Využívání společné komunikační infrastruktury a sdílení komunikačních médií.

- **Administrativní budova**



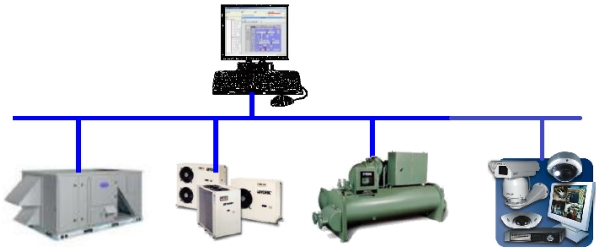
Obr. 10. Priority funkcí administrativní budovy [32].

- **Chráněná budova**



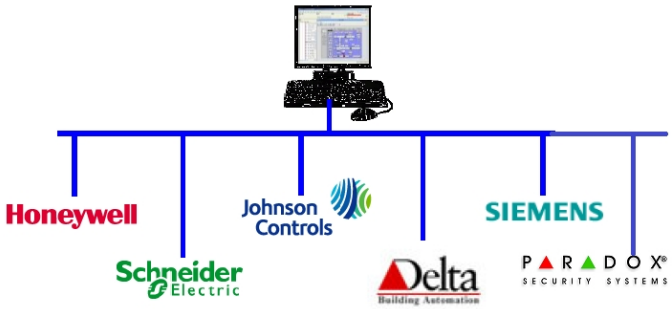
Obr. 11. Pririty funkcí chráněné budovy [32].

Integrované poplachové systémy a další řídicí systémy lze rozdělit podle **různých subsystémů**, které jsou vzájemně propojeny a jsou schopné si vzájemně předávat informace.



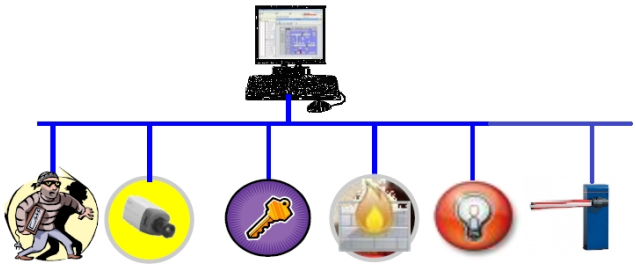
Obr. 12. Integrace sub-systémů[32].

Integrovat lze systémy od **různých dodavatelů**, kteří musí vyrábět produkty využívající společné komunikační protokoly. Ostatně o samotnou komunikaci se starají integrační zařízení a softwary, které mají ve své hlavní funkci zpracovávat a spravovat datový tok informaci v systému.



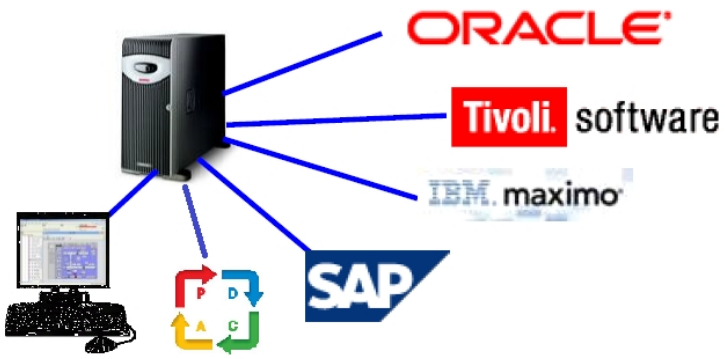
Obr. 13. Integrace různých dodavatelů [32].

Další strukturu integrace lze chápat jako propojení **různých aplikací**. Vzájemné ovlivnění svých funkcí, záleží na konkrétních požadavkách struktury a účelu budovy.



Obr. 14. Integrace různých systémů [32].

Nejvyšší stupeň provázání jednotlivých aplikací je integrace se **systémy řízení podniků**. Zde jsou požadavky soustředěny převážně strukturu administrativní budovy, které zpracovávají osobní informace svých zaměstnanců například mzdový systémy.



Obr. 15. Integrace se systémy řízení podniků [32].

Hlavním důvodem propojení jednotlivých systémů je vzájemné sblížení a sloučení funkcí použitých aplikací. Využívání otevřených standardu pro komunikaci umožňuje konvergenci využívaných systémů.

Integrovaná platforma systému moderních budov vychází z používaných aplikací, které společně tvoří řídicí systémy. Platforma se skládá z následujících odvětví:

- **slaboproudé systémy**,
  - bezpečností systémy,
    - PZTS,
    - CCTV,
    - ACS,
    - SAS,
  - protipožární systémy,
    - elektrická požární signalizace,
    - nouzový a evakuační rozsah,
    - samočinné hasicí zařízení,
  - systémy provozu budov,
    - docházkové a stravovací systémy,
    - strukturovaná kabeláž,
    - telefonní ústředna,
    - informační systémy,
    - datové sítě,
    - ozvučení,
    - systém jednotného času,

- **ostatní systémy / technologie**,
    - počítačové sály,
    - správa údržby,
    - správa energetických toků,
    - technická zařízení budovy,
        - vzduchotechnika / klimatizace / vytápění,
        - zdroje tepla, chladu a akumulace,
        - zdroje elektrické energie / nouzové napájení / osvětlení [32].

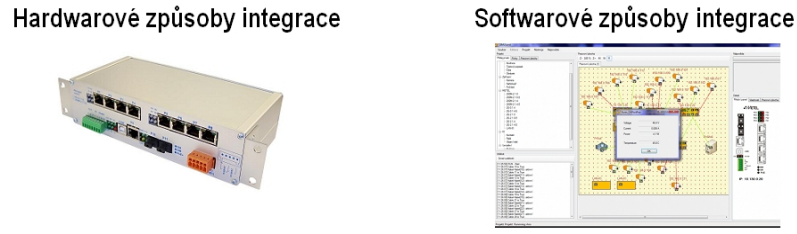
3.1.2 Způsoby propojení

Základním principem integrace poplachových systémů představuje efektivní způsob využití současných technologických možností prvků zabezpečovacích, kamerových, přístupových a tísňových systémů. Jednotlivé předchozí aplikace je možno propojit navzájem nebo je zde možnost doplnit o nepoplachové systémy. Tím docílíme zjednodušení automatizačních procesů v komerčních i rezidenčních objektech.

Jednotlivé **formy integrace** poplachových i nepoplachových aplikací lze rozdělit na:

- **technologická integrace** – vzájemné propojení PZTS, CCTV, ACS, SAS + řízení osvětlení, vytápění,
- **funkční integrace** – vzájemné sjednocení funkcí přístupových karet: evidence vstupu/ evidence výrobních operací,
- **integrace uživatelského rozhraní** – sloučené ovládání poplachových a nepoplachových aplikací (ovládací panely, SW pro mobilní telefony/tablety)
- **datová integrace** – data využívající SW produkty k zabezpečení identifikace, evidence vstupu a docházky osob → mzdový systém,
- **metodická integrace** – metodika zabezpečení registrace a pohybu návštěv, osob, vozidel, možná blokace vstupů[8].

Technické způsoby vzájemného propojení jednotlivých aplikací, lze rozdělit na dvě základní skupiny uvedené níže na obrázku.

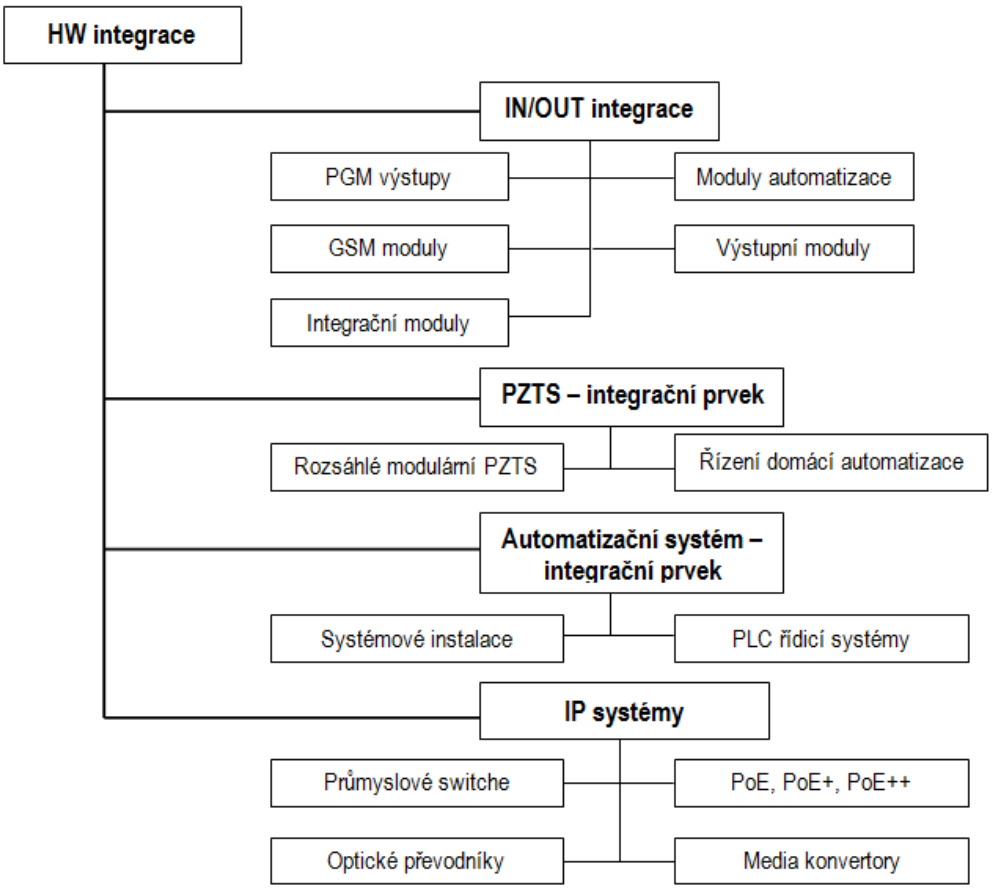


Obr. 16. Technické způsoby integrovaných systémů.

HW integrace

Technické možnosti hardwarová integrace poplachových a nepoplachových aplikací vychází ze vzájemného propojení vstupů a výstupů jednotlivých systémů. Dalším specifikem jsou technické parametry poplachových zabezpečovacích systémů, kde případné specifické zpracování informace je vyřešeno pomocí rozšiřujících modulů.

K hardwarovým způsobům integrace je možno zařadit i automatizační systémy (programovatelné automaty, systémová elektroinstalace), které mimo ovládaní standardních technologii v budovách nabízí možnost připojení zabezpečovací prvků.



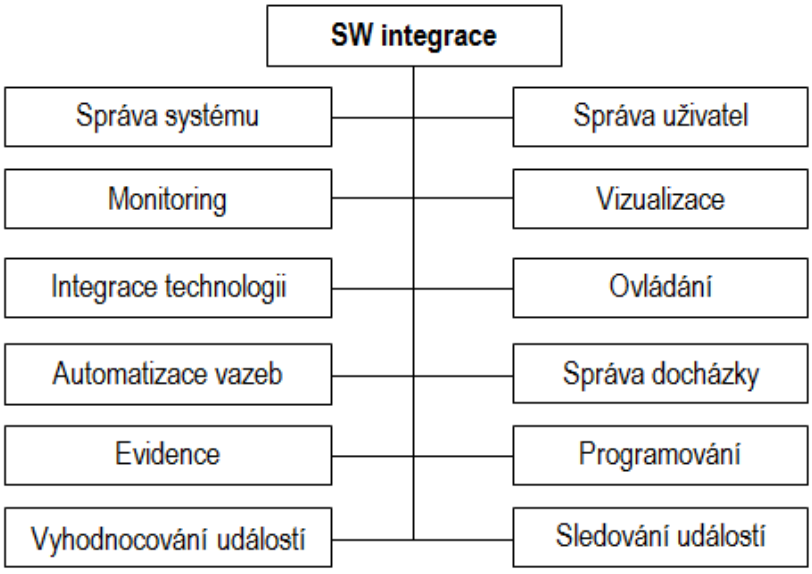
Obr. 17. Rozdělení HW integrace [8], upravil Macháč 2013

SW integrace

Softwarové (SW) způsoby integrace poplachových a nepoplachových aplikací vychází ze vzájemného **propojení** samostatných **aplikací** prostřednictvím komunikačního media. SW integrace se využívá pro ovládání, správu, vizualizaci digitálních vstupů a pro další funkce prvků rozšiřující nadstavbové SW produkty, které mohou být použity na externím počítači (servery, klientská PC) nebo autonomní řídící centrále s odpovídajícím SW zařízením.

Nejvyšší stupeň SW integrace poplachových a nepoplachových aplikací vychází z propojení komunikačních zařízení k serveru prostřednictvím sítí (LAN, WAN) [8].

Nadstavbové SW produkty je možno klasifikovat podle funkcí.



Obr. 18. Funkce SW integrace [8].

Uvedené funkce v předchozím obrázku v sobě zahrnují integraci vybraných činností nebo technologii například formou vytváření centrálních databází pro správu uživatelů, centrální vizualizace nebo nastavení automatických vazeb mezi propojenými systémy.

3.2 Metody integrace pomocí prvků informační technologie

V dnešní době existuje velké množství firem zabývající se výrobou integrovaných systémů. Jak bylo výše uvedeno integraci lze rozdělit na vrstvy vzájemného propojení jednotlivých subsystémů. U každého návrhu integrovaného poplachového systému vycházíme z požadavků zákazníka. Dle stanovených požadavků, můžeme vybrat optimální integrovaný

systém. Následující obrázek představuje loga výrobců integrovaných poplachových systémů na našem trhu.

Obr. 19. Výrobci integrovaných systémů.

Následující část práce představuje analýzu **technických možností** integrace poplachových systémů s využitím prvků informační technologie. Budou následně popsána jednotlivá zařízení, kde jejich hlavní prioritou jsou **poplachové aplikace** využívající informační technologii.

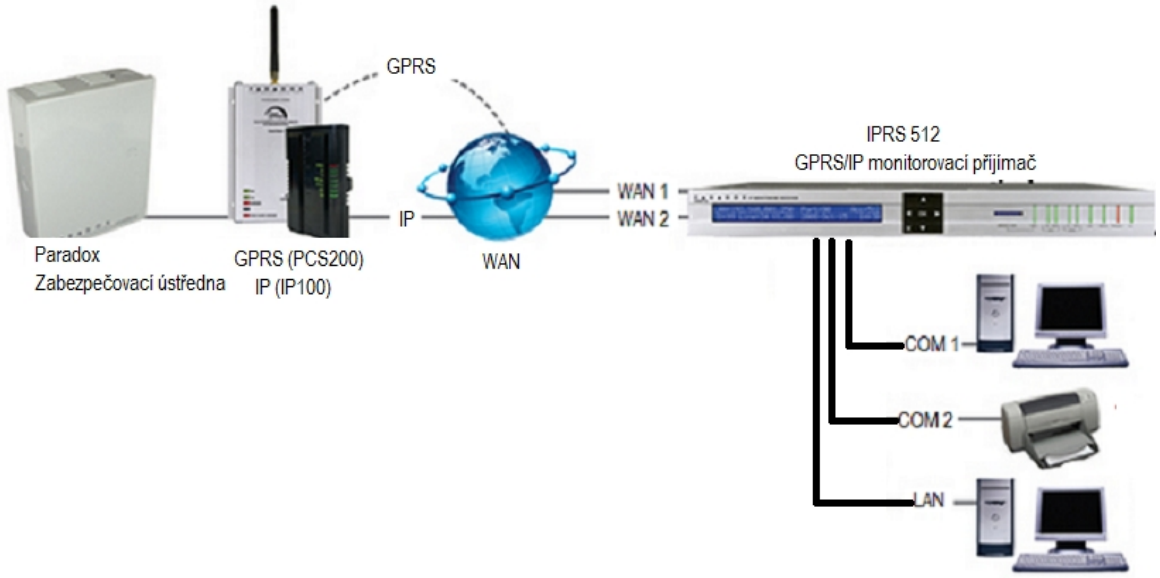
3.2.1 Paradox

Všechny ovládací zařízení od firmy Paradox byly speciálně postaveny od základu tak, aby podporovaly komunikační technologie (**GPRS, GSM, IP a hlas**). Zařízení se využívají při nahrávání/stahování přes GPRS, monitoring a ovládání systému na dálku pomocí PC, vyhodnocení stavu a události hlasové nebo textové zprávy.

Centrálním prvkem integrovaného systému využívající prvky informační technologie, je monitorovací přijímač IPRS512. Zařízení IPRS512 zpracovává informace z IP a GPRS komunikačních sítí. Pro zabezpečený přenos dat používá šifrovací algoritmus **AES** 256 – bit. Pro přenos dat ze zabezpečovací ústředny se využívají integrující moduly pro GPRS (**PCS200**) a pro IP (**IP100**). Na monitorovací přijímač IPRS512 může mýt připojených až 512 integračních modulů.

Komunikace mezi IPRS512 a dohledovým poplachovým přijímacím centrem využívá formátu MLR2, Radionics 6500, Ademco 685. V integrovaném systému lze využívat systémy: Digiplex EVO, Magellan, Spectra, E55/65 Ultra 728. IPRS512 podporuje softwary WinLoad, In-Field, NEware.

Následující obrázek představuje možnost přenosu poplachové i nepoplachové informace z připojených systémů s využitím prvků informačních technologií od firmy Paradox.



Obr. 20. Příklad přenosu poplachové i nepoplachové informace s využitím prvků informačních technologií [33].

Technické parametry IPR512:

- připojení do 512 bezpečnostních systémů Paradox,
- podporuje CID a SIA formáty
- 256-bit AES šifrování dat,
- 40-znakový LCD, pro informační stavy zařízení, zálohování dat,
- nastavená IP adresa a maska podsítě pro LAN port,
- Velikost zařízení 19´´
- 2 x WAN (WAN1,WAN2),
- 2 x COM,
- napájení 110/220V,
- nízká spotřeba (do10 W) [33].

3.2.2 Johnson Control

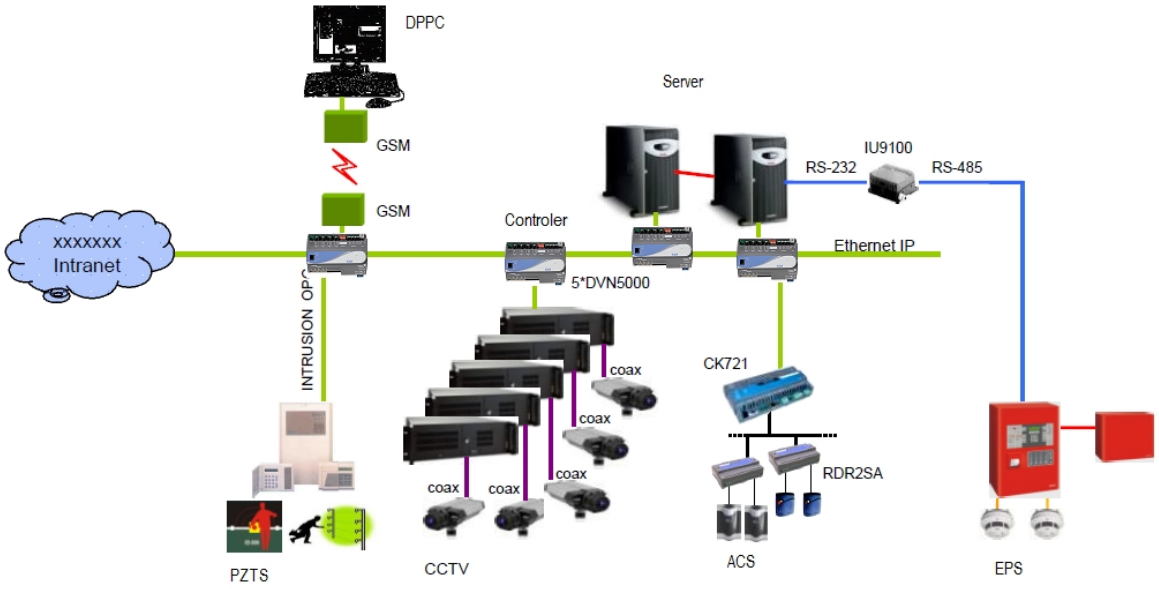
Vychází z široké nabídky integrovaných systémů, které lze využít ve zdravotnictví, školství, státní instituci, dopravě a dalších komerčních i objektech. Při integraci poplachových systémů s využitím prvků informační technologie využívá kontrolér, na které jsou připojeny IN/OUT moduly a další zařízení dle požadavků na funkčnost. Kontroléry jsou připojeny na

řídící jednotku, která odesílá data na dispečerské pracoviště s nadstavbovým softwarem pro ovládání, monitorování a kontroly stavů jednotlivých zařízení.

Koncepce integrovaného systémů vychází z **building management system (BMS)** – následující obrázek představuje role řídicího systému budov.

Obr. 21. Role BMS [34].

Při integraci poplachových systému propojuje vzájemně zabezpečovací, kamerové, přístupové a elektrické požární systémy. Z řady zabezpečovacích systémů jsou použity ústředny Galaxy Dimension včetně RFID perimetrického systémů. Následující obrázek představuje možnost integrace poplachových systémů.



Obr. 22. Příklad Integrace poplachových systémů od firmy Johnson Control [32].

Technické parametry přístupového kontroléru S321 –IP:

- vstupní napětí 12 – 24VDC,
- až 5000 uživatelů,
- 4 MB flash paměti,
- připojení k síti 10/100Base-T,
- aktualizace pomocí File Transfer Protocol (FTP),
- nastavení rozvrhu, zálohování dat [34].

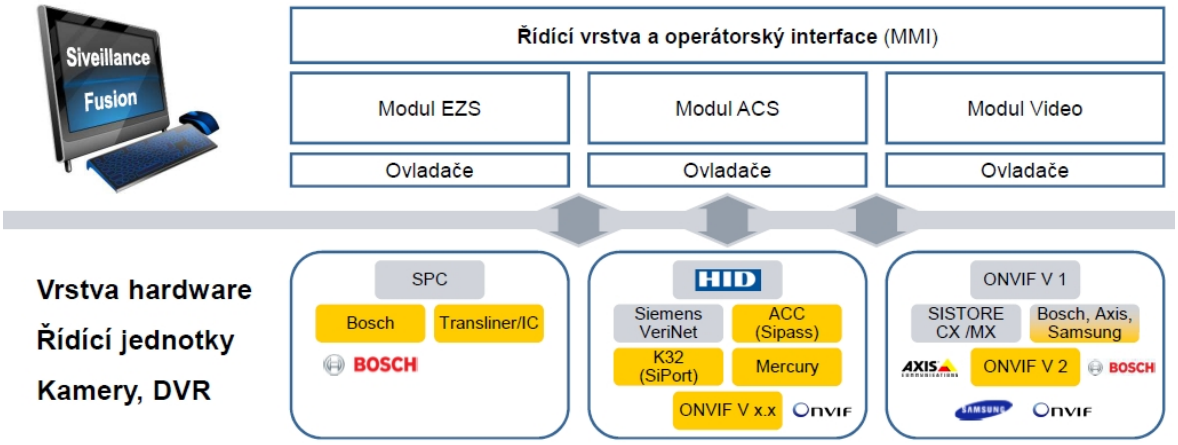
3.2.3 Siemens

Integrované systémy od firmy Siemens jsou založený na funkcích snižování energetické náročnosti budovy, elektrickém požárním, zabezpečovacím a geografickém systému.

Integrace poplachových systémů vychází převážně z propojení systému kontroly vstupu, průmyslové televize, poplachového zabezpečovacího a tísňového systému a elektrické požární signalizace. Integrované systémy lze využít v oblastech uvedené na obrázku.

Obr. 23. Oblasti nasazení integrovaných systémů [35].

Jako příklad pro velké společnosti uvedu systém Siveillance Fusion, které propojuje funkce jednotlivých subsystémů následujícím způsobem uvedeným na obrázku.



Obr. 24. Systém Siveillance Fusion od firmy Siemens [35].

Komunikace probíhá pomocí integračního rozhraní mezi jednotlivými aplikacemi. Bezprostředně pro správnou komunikaci je využíváno standardizovaných komunikačních protokolů.

Řídící stanice **MM8000** využívá moderní softwarové řešení Siveillance Fusion a síťové technologie, které jsou vytvořeny pro účely bezpečnostních aplikace. Technické parametry MM8000:

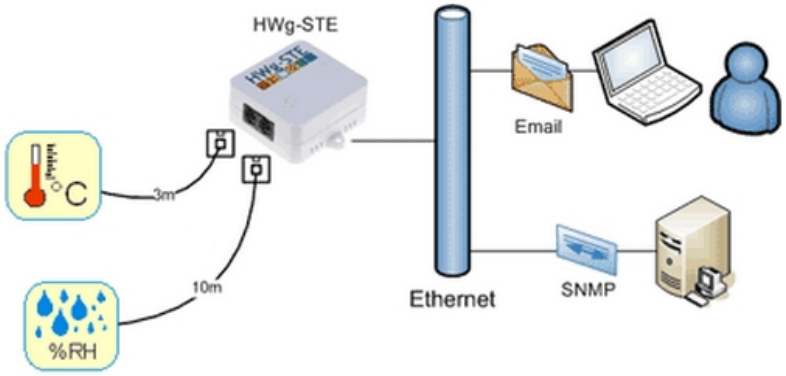
- operační systémy Windows XP/7,
- formáty BACnet, OPC,
- SQL server,
- podpora AutoCAD,
- maximální počet je 150 DVR,
- maximální počet zařízení využívající BACnet je 64 zařízení [36].

Prvky pro přenos dat/videosignálu:

- přenos po koaxiálním kabelu,
- přenos po krouceném páru,
- optické převodníky,
- rádiové přenosy,
- Web servery,
- pomocí LAN.

3.2.4 HW Group

Integrované systémy od této firmy podléhají spíše požadavkům na nepoplachové aplikace. Snaží se vývoj obohatit o poplachové aplikace, které budou navazovat na stávající integrovaný systém. V dnešní době lze tyto integrované systémy instalovat tam, kde je zvýšené riziko zaplavení hlídaného místa. Zajišťuje sledování přehřátí technologii (server, disková pole). Dohled teploty v lednicích a chladicích boxech, kde senzory reagují na vlhkost, otevření dveří nebo atmosférický tlak, využívají se pro optimalizaci podmínek skladování potravin nebo léčiv. Následující obrázek představuje využití ethernet teploměru HWg-STE [37].



Obr. 25. Integrace nepoplachových aplikací (HW Group) [37].

Webový teploměr se nastavuje přes zabudovaný web server. Pokud je měřená veličina (teplota/vlhkost) nad nastavený limit pošle email s upozorněním. Obsahuje software pro zobrazení grafu a export dat do MS Excelu. Při použití zařízení I/O Controller lze ovládat vzdáleně sepnutí relé po síti LAN, umožňuje tím vypnout/zapnout jakékoliv zařízení.

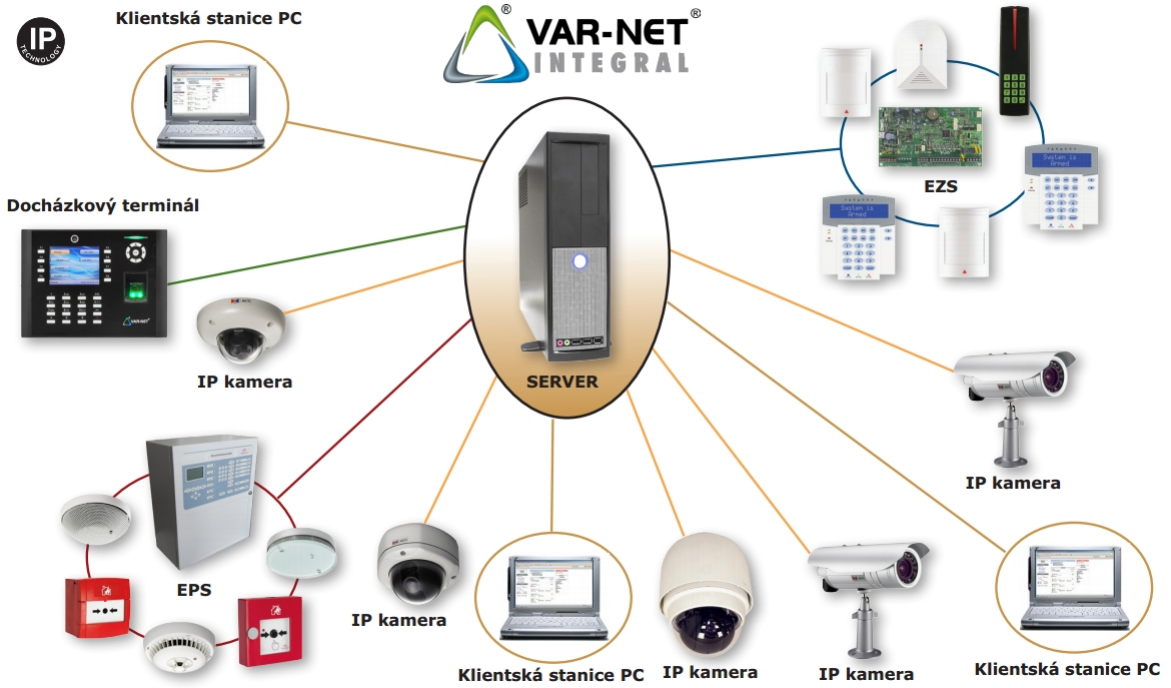
Technické parametry HWg – STE:

- vestavěný WEB server,
- ethernet: 100Mbit,
- IP protokoly: ARP, TCP/IP (HTTP, NTP, SMTP), UDP/IP (SNMP)
- podporuje DHCP,
- M2M protokoly: XML,http, SNMP,
- napájení: 5V / 1W [37].

3.2.5 Variant

Variant s externí firmou vytvořili integrační software VAR-NET INTEGRAL pro monitorování, správu a vyhodnocování stavu elektrických systémů budov. Umožňuje z jednoho místa přes webové rozhraní spravovat a ovládat více vzdálených objektů. Modularita systému slouží k zefektivnění používání SW, vždy budou použity jen ty funkce, které budou použité k běžnému provozu. Do SW VAR-NET INTEGRAL lze připojit:

- zabezpečovací ústředny - Digiplex Evo, Galaxy,
- kamerové systémy – IP kamery ACTi, DVR Micro Digital, AXIS
- elektrické požární signalizace – JOB detectomat , SIEMENS
- docházkové a přístupové terminály – VAR-NET [38].



Obr. 26. VAR-NET INTEGRAL [38].

K propojení zařízení se serverem využívají integračního modulu PRT3, tento integrační modul slouží i jako doplňkové zařízení k převodníku GNOME323, který komunikuje se zabezpečovací ústřednou přes RS232. Security View je vizualizační SW speciálně určený pro zabezpečovací ústředny.

Technické parametry PRT3:

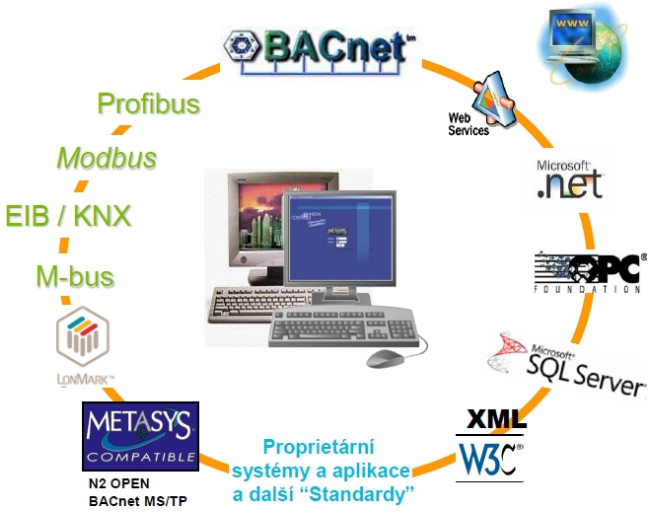
- jedinečné sériové číslo,
- napájení: 11 – 16 VDC
- proudový odběr: max. 60 mA,

- paměť EEPROM,
- datový výstup/vstup: ASCI/E-BUS,
- paralelní port, sériový port, USB port,
- paměť událostí [38].

3.3 Společné protokoly

Nejdůležitějším prvkem propojení různých zařízení do jednoho integrujícího systému, se stávají komunikační protokoly. Jednotlivá zařízení využívající se v integraci poplachových systémů mají určené komunikační protokoly výrobcem. **Komunikace** může probíhat v integrovaném systému na **úrovni jednoho protokolu**, kde výrobci prosazují koupi dalších svých zařízení. Nevýhoda v tomto směru je, že každý výrobce nemusí mít v nabídce speciální poplachové zařízení, dle požadavků klienta. Výhoda přichází v okamžiku propojení, kde komunikace a vzájemné ovlivnění zařízení bude probíhat na nejvyšší úrovni. Další možností komunikační úrovně je využití **více protokolů** v integraci poplachových systémů. Výhoda je spojena s využití většího množství speciálních zařízení, které podporují odlišné komunikační protokoly. Nevýhoda je v důsledku využívání vice komunikačních protokolů, způsobena možností negativního ovlivnění jednotlivých příkazů.

Předcházení negativního ovlivnění komunikačních protokolů zajišťují otevřené standardy, které umožňují konvergenci jednotlivých funkcí systémů. Následující obrázek představuje přehled komunikačních protokolů.



Obr. 27. Standardy a protokoly [32].

Každý komunikační protokol je vhodný pro určité použití různých poplachových aplikací. Hlavním faktorem správného zvolení komunikačního protokolu je výsledný formát, ve kterém jsou aplikována data. Pro periodické sledování hodnot všech akčních členů jsou určeny protokoly **otázka-odpověď**. Pracují v režimu TCP Server, kde čekají ma oslovení z nadřízené aplikace.

WEB – HTML (WWW stránka)

Jednotlivé akční stavy jsou zobrazovány na WWW stránce, která je vytvořena tak, aby splňovala požadavky zákazníka. Přístup lze omezit použitím filtru IP adres. Využití tohoto protokolu je u menší a středních objektů pro okamžitou signalizaci stavů systému.

HTTP – XML tagy

Všechny aktuální snímané hodnoty ze senzorů jsou zobrazeny v definované .XML stránce. Jakákoliv aplikace může hodnoty načítat z XML tagů. Pro TCP/IP komunikaci (Mashine-to-Mashine) se jedná o nejefektivnější způsob vyčítání všech hodnot zároveň, jelikož jsou v jednou souboru uloženy všechny hodnoty ze senzorů.

Modbus

Komunikační protokol souží pro měřící zařízení, využívající ke komunikaci RS-485/RS-323. Modbus se využívá pro sdílení po jednom z fyzických rozhraní celou paměťovou oblast proměnných veličin. Modbus/TCP protokol je rozšířen o komunikaci pomocí Ethernet. Výhodu představuje snadné použití do vizualizačních systémů v průmyslovém odvětví.

SNMP

Protokol SNMP (Simple Network Management Protocol) se využívá k přenosu základních systémových informaci pomocí krátkých paketů. Všechny proměnné veličiny jsou uspořádány a popsány v MIB (Management Information Base) tabulce, které je přiřazena k určitému zařízení. V tabulce je uveden identifikátor proměnných OID (Object Identificator), které představuje dlouhé číslo pro definici pozice ve struktuře stromu proměnných. Komunikační protokol se využívá pro telekomunikace a vzdálenou správu [39].

BACnet

Komunikační sběrnice BACnet (Building Automation and Control Network) byla vytvořena na základě využití internetových protokolů v oblasti automatizaci budov. Podporuje tedy IP

(Internet Protocol) a umožňuje tímto způsobem využívat globální síťové systémy. Využívá se převážně na analogové hodnoty a dvoustavové vstupy/výstupy, ovládání, plánování, tedy hlavní prioritou protokolu je většinou monitorování a řízení systémů a aplikací budov. BACnet není klasickým komunikačním protokolem, ale dá se říct, že kontroluje jen vyšší vrstvy komunikačního modelu a na nižší úrovni využívá stávající komunikační systémy (TCP/IP, RS-485) [40].

M-Bus

M-Bus (Meter-Bus) se řadí mezi průmyslové komunikační protokoly určený především pro vzdálený odečet hodnot z měřičů spotřeby, kde je nejdůležitější odolnost vůči vnějšímu rušení a na rychlosti přenosu příliš nezáleží. Využívá asynchronní sériové 8-bitové komunikace (RS-323), kde jednotlivé strany posílají ucelené rámce s daty[41].

KNX/EIB

Evropská instalační sběrnice KNX/EIB je průmyslový komutační systém, který se používá v systémové technice budov pro síťové informatické spojení zařízení. Přenos dat pro vzájemnou komunikaci se ukládají do datového telegramu a pomocí instalační sběrnice se digitálně přenášejí. Sběrnici lze realizovat různým fyzikálně-technickým způsobem (KNX/TP-kroucený pár, KNX.PL-silový kabel, NX.RF-bezdrátový přenos). KNX/EIB se používá například pro realizaci ovládání a řízení osvětlení a nastavení žaluzii a dalších technologii využívajících se u komerčních systémů [42].

Dílčí závěr

Použití integrovaného poplachového systému si vyžaduje profesní přístup od samého začátku konzultace se zákazníkem až po ovládání jednotlivých uživatelů. Požadavky na integrované systémy se budou více zpřísňovat, protože každý uživatel by chtěl mít všechny zařízení v jednom ovládacím rozhraní. Proto výrobci integračních systémů se snaží rozšiřovat své pole působnosti a díky tomu oslovit větší škálu zákazníků. Jestli to brát jako výhodu nebo nevýhodu je otázkou. V dnešní době je možná také výhodnější vsadit na jeden aplikační obor, ve kterém bude systém nejspolehlivější a dokáže konkurovat dalším výrobcům integrovaných poplachových systémů.

PRAKTICKÁ ČÁST

4 NÁVRH INTEGROVANÉHO SYSTÉMU

V praktické části diplomové práce se budu zabývat návrhem integrovaného poplachového systému s využitím prvků informačních technologií. Integrovaný systém bude navržen pro modelový příklad **průmyslového objektu**, který se skládá z výrobní a administrativní budovy. Samotný návrh představuje soubor činností, tvořící první část etapy procesu zřizování integrovaného poplachového systému. Cílem soustavných činností je zpracování výstupního dokumentu – Návrh skladby systému, zkráceně označován jedním slovem jako Návrh. Jednotlivé dílčí etapy návrhu představují:

- stanovení rozsahu IPS,
- volbu komponent,
- zpracování návrhu systému [20].

Účastníci, kteří se budou podílet na účelném zpracování a ovlivnění návrhu jsou: **objednavatel** (investor, zadavatel, uživatel), **dodavatel** (řešitel, projektant, obchodní společnost), **provozovatel**. Další potenciálně dotčené subjekty návrhu systému jsou pojišťovny, Policie ČR, bezpečnostní agentury, provozovatelé telekomunikačních systémů.

Základní činnost etapy **návrhu** IPS obsahuje především bezpečnostní posouzení objektu a vlivů působících v daném prostoru. V následující tabulce je přehled všech základních činnostní a dokumentů využívaných při návrhu systému:

Tab. 4. Činnosti a dokumenty při návrhu systému [20].

Činnost	Dokumentace
Analýza potřeb zákazníka	Zápis jednání se zákazníkem
Bezpečnostní posouzení objektu	Zápis o bezpečnostním posouzení objektu
Posouzení vlivů působících na objekt	Zápis o stanovení vnějších vlivů
Zpracování technické specifikace systému	Nabídka s konkrétním technickým řešením. Návrh skladby systému
	Návrh smlouvy o dílo (objednavatel/zhotovitel)

Uvedené činností etapy návrhu systému se mohou vzájemně překrývat a splývat dle stanoveného rozsahu zakázky. Tím pádem u jednodušších realizací může návrh skladby systému obsahovat rovnou projektovou dokumentaci (plán montáže), každá prováděná činnost je třeba zdokumentovat, dle stanoveného rozsahu IPS a stupni zabezpečení objektu.

Při návrhu systému vycházíme z těchto obecných zásad:

- při zpracování návrhu je důležité se dívat na objekt očima potencionálního pachatele,
- v závislosti na míře rizika volit příslušné komponenty,
- zohlednit požadavky vycházející z bezpečnostního posouzení,
- různé objekty lze zařadit do stejné míry rizika, jen s rozdílem počtu nasazení komponent, umístění komponent, jejich kombinace a zálohování přenosových cest,
- zohlednění specifik požadavků na obsluhu systému,
- zvážení možnosti integrace s nepoplachovými systémy [20].

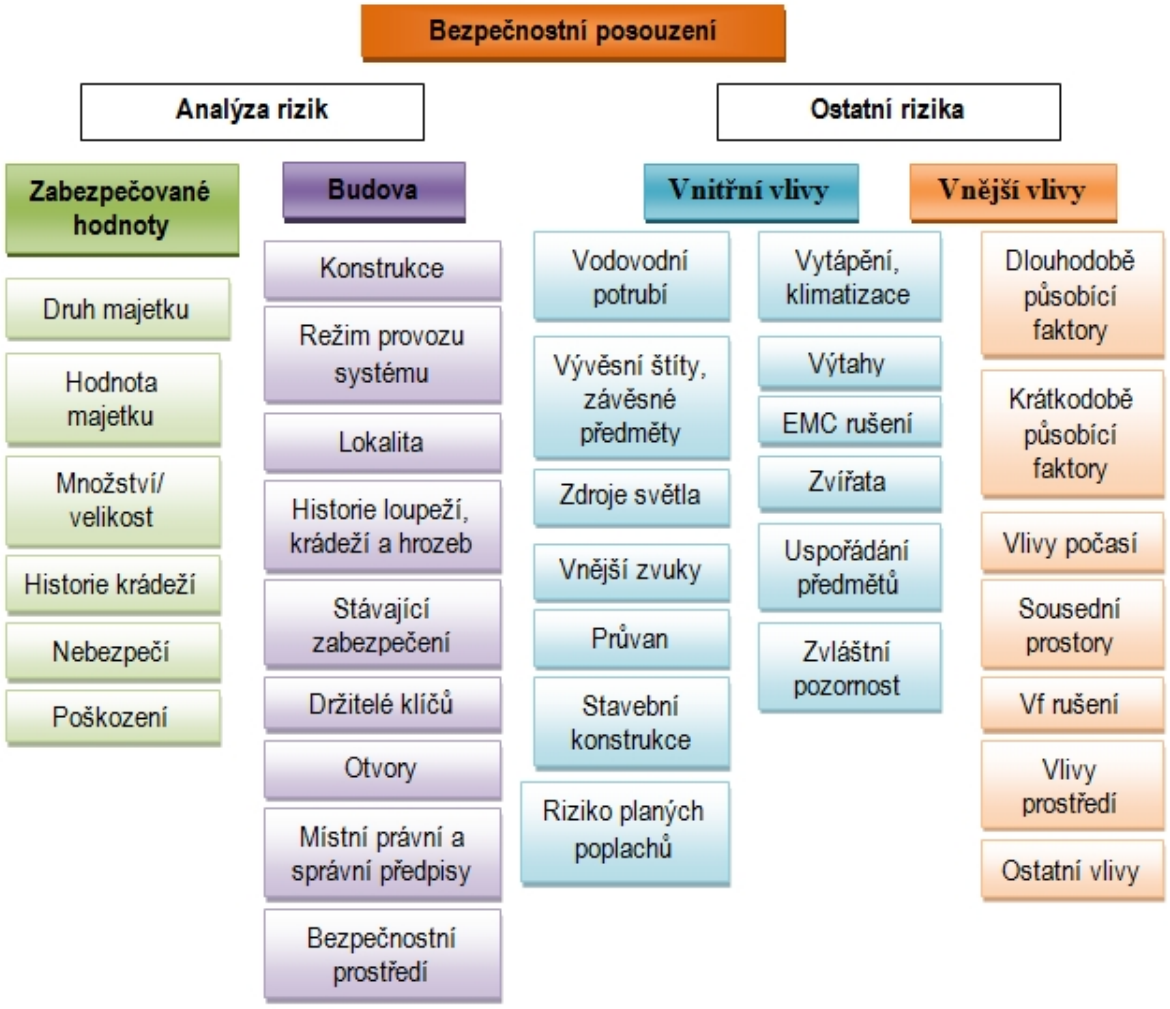
Bezpečnostní posouzení objektu

Bezpečnostní posouzení objektu z hlediska nasazení integrovaného poplachového systému je možno definovat jako **proces analýzy faktorů ovlivňujících návrh** poplachových aplikací. V rámci bezpečnostního posouzení se snažíme vycházet v průběhu přípravy systémového návrhu, faktory mající určitý vliv na správnou volbu komponentů a jejich umístění.

Dalším důležitým faktorem je stanovení požadovaného stupně zabezpečení.

V průběhu procesu zřizování integrovaného poplachového systému představuje bezpečnostní posouzení a konzultace s účastníky objektu první krok v návrhu systému. Bezpečnostní posouzení objektu je založeno na výsledku čtyř základních oblastí zájmu: zabezpečované hodnoty, budovy, vnějších a vnitrních vlivů [20].

Náplň jednotlivých oblastí bezpečnostního posouzení popisuje následující obrázek.



Obr. 28. Oblasti bezpečnostního posouzení objektu [20], upravil Macháč 2013

Analýza rizik stanovuje posouzení zabezpečených hodnot a budovy, je zpracována v důsledku určení požadovaného stupně zabezpečení dle ČSN EN 50131-1 ed.2. Ostatní rizika tvoří vnitřní a vnější vlivy, které působí na komponenty IPS. Stupeň zabezpečení objektu se určí dle předpokladů znalostí a technických možností potenciálního pachatele.

4.1 Návrh skladby systému

Dokument **návrh** systému IPS **slouží** v rámci nabídkového řízení k úspěšnému **sestavení rozpočtu** dodávky a jako **podklad** k jednání se zákazníkem. Dále jsou nedílnou součástí podkladu pro tvorbu projektové dokumentace.

Body návrhu skladby systému prakticky popisují vybrané činnosti, stanovené v bezpečnostním posouzení objektu. Jednotlivé kroky musíme realizovat a následně zpracovat do návrhu, určující volbu typu ochrany, stanovení třídy prostředí, volba komponent, stanovení způsobu signalizace.

4.1.1 Údaje o klientovi

Adresa: STAV GROUP, a.s.
Kojetínská 5555 /54, 755 22
Přerov I-Město

Telefon: +420 581 555 444

4.1.2 Údaje o střeženém objektu

Objekt se nachází na adrese: STAV GROUP, a.s., Kojetínská 5555/54, 750 02, Přerov I-Město. Obchodní společnost STAV GROUP, a.s. lze zařadit do kategorie: pronájem výrobních, skladovacích a kancelářských prostor.

Objekt se skládá z výrobní haly a administrativní budovy. Výrobní hala je rozdělená na jednotlivé výrobní úseky, které si pronajímají externí firmy na svou výrobní činnost. Administrativní budova nabízí pronájem kancelářských prostor pro výrobní firmy.

Tab. 5. Charakteristika meteriálů objektu.

Charakteristika	Výrobní hala	Administrativní budova
Umístění objektu	Zvýšené přízemí	Sklep, suterén, druhé a další nadzemní podlaží
Konstrukce objektu	Zděný	Zděný
Konstrukce příček	Ocelové sloupy	Zděné
Vstupní dveře a vrata	Kovové	Kovové/prosklené
- dveřní mechanizmus	Bez vnější kliky, elektronický zámek	Bez vnější kliky, elektronický zámek, autom. zavírání
- klíče	Sektorové	Sektorové, univerzální
Okna	Kovová	Kovová/plastová s mřiží v přízemí
Ostatní otvory	Světlíky, odpadní šachty, technologické otvory, ventilace	Světlíky, odpadní šachty, technologické otvory, ventilace

Účel využití objektu je směřován do strojírenského odvětví. Výrobní hala nabízí provozní jeřáb, pro každý provozní sektor. Firmy sídlící ve výrobní hale se soustředí od zpracování bronzových součástek, po výrobu konstrukčních prvků pro různé stavby od mostů po velké haly.

4.1.3 Stupeň zabezpečení

Stupeň navrženého zabezpečení poplachového zabezpečovacího a tísňové systému se zvolí na základě bezpečnostní posouzení objektu. Je určený **2. stupeň** zabezpečení, kde se předpokládá, že potencionální narušitelé nebo lupiči mají omezené znalosti PZTS a používají základní sortiment běžného nářadí a přenosných přístrojů.

PZTS může obsahovat prvky různých stupňů zabezpečení za předpokladu, že je rozdělen na více jednoznačně definovaných subsystémů. Stupeň zabezpečení subsystému je dám tím prvkem subsystému, který má nejnižší stupeň. Prvky, které slouží jako společné zařízení pro více subsystémů, musí mít stupeň zabezpečení stejný jako je nejvyšší stupeň subsystému.

4.1.4 Třída okolního prostředí

Při předpokládaném umístění jednotlivých prvků IPS, musíme vycházet ze stanovení požadavků na třídu prostředí, ve kterém budou jednotlivé komponenty systému instalovány. V objektu **administrativní budovy** se bude jednat převážně o **třídu prostředí I. a II.,** na prvky instalované na **plášť budovy** bude příslušná **třída prostředí III**. V objektu **výrobní haly** budou použité komponenty IPS podléhat do **třídy prostředí II. a III.** Prvky používané u **perimetrického zabezpečovacího** systému budou určeny **IV. třídou prostředí**.

Třídy prostředí jsou uvedeny v následující tabulce.

Tab. 6. Určení třídy prostředí nasazení komponentů [20].

Třída prostředí	Název	Popis prostředí	Rozsah teplot
I.	Vnitřní	Vlivy prostředí vyskytující se obvykle ve vnitřních prostorách při konstantní teplotě (obytné nebo obchodní prostory).	+5°C až + 40°C
II.	Vnitřní všeobecné	Vlivy prostředí vyskytující se obvykle ve vnitřních prostorách, kde není stálá teplota (chodby, haly, schodiště, nevytápěné skladové prostory).	-10°C až + 40°C
III.	Venkovní chráněné	Vlivy prostředí vyskytující se obvykle vně budov, přičemž komponenty IPS nejsou plně vystaveny povětrnostním vlivům.	-25°C až + 50°C
IV.	Venkovní všeobecné	Vlivy prostředí vyskytující se obvykle vně budov, přičemž komponenty IPS jsou plně vystaveny povětrnostním vlivům.	-25°C až + 60°C

Jednotlivé prvky IPS musí správně fungovat, jsou-li vystaveny působením vlivů určeného prostředí I. – IV. třídy. Stanovené požadavky na zařízení mají vzrůstající tendenci dle určené třídy prostředí. Tedy zařízení vyhovující třídě IV. lze použít i ve všech třech předchozích třídách prostředí.

4.1.5 Seznam materiálu

Tato část dokumentu obsahuje přehled zařízení, které budou použity při integraci poplachových systému. Zařízení sloužící k integraci poplachových systému s využitím prvků informační technologie, jsou zvoleny komponenty od české firmy **METEL s.r.o**.

Firma Metel začínala s vývojem a výrobou vlastních výrobků z oblasti přenosových systémů. Na začátku začínali s výrobou zesilovačů, oddělovačů, posléze úspěšných optických převodníků, až po dnešní **nejmodernější IP produkty**, vyhovující evropským harmonizovaným normám. Všechna zařízení, která vyrábí, jsou testované a certifikované inspekčním úřadem TÜV a dalších zkušebnách pro zabezpečovací, požární a další druhy poplachových i nepoplachových systémů.

Při výběru vhodného integrovaného poplachového systému s využitím prvků informační technologie vycházíme z požadavků majitele a provozovatele. Ve výsledku celého návrhu se snažíme docílit snížení provozních nákladů a efektivního využití použitého systému.

Pomocí integrace systémů docílíme propojení funkcí poplachových aplikací. Integrovaný systém bude obsahovat propojení:

- poplachového zabezpečovacího a tísňového systému,
- přístupového systému,
- perimetrického systému,
- kamerového systému.

Při návrhu musíme zvolit jaký hardwarový a softwarový způsob použijeme na propojení jednotlivých poplachových aplikací.

4.1.5.1 Poplachový zabezpečovací a tísňový systém

Integrační komponenty od firmy Metel podporují velké množství bezpečnostních ústředen. Pro zvolený objekt jsem vybral ústřednu od firmy **Honeywell**, přehled použitých zařízení najdete v následující tabulce.

Tab. 7. Použité prvky PZTS.

Zařízení	Název/Typ	Počet kusů
Ústředna	Galaxy DimensionGD - 520	1
Pohybový detektor	PIR detektor IS2560T Honeywell	29
Detektor otevření	Mag. kontakt vratový EMPS50	6
	Mag. kontakt na dveře/okna MC2110C	25
Signalizační zařízení	Zálohovaná siréna Risco RS200W	2
Ovládací zařízení	Dotyková klav. Honeywell CP041	1
	LCD klávesnice Honeywell MK7	1

U 2. stupně zabezpečení jsou požadavky kladeny na detekci otevření obvodových dveří, oken a ostatních otvorů. Místností musí být střeženy pohybovým detektorem, v nichž je vysoké riziko narušení.

4.1.5.2 Přístupový systém

Nejvhodnější varianta přístupového systému je nadstavbový přístupový systém, k řadě zabezpečovací ústředny Galaxy Dimension. Jedná se o **rozšíření funkcí** zabezpečovací ústředny pomocí řídících modulů, na které lze připojit bezkontaktní čtečky.

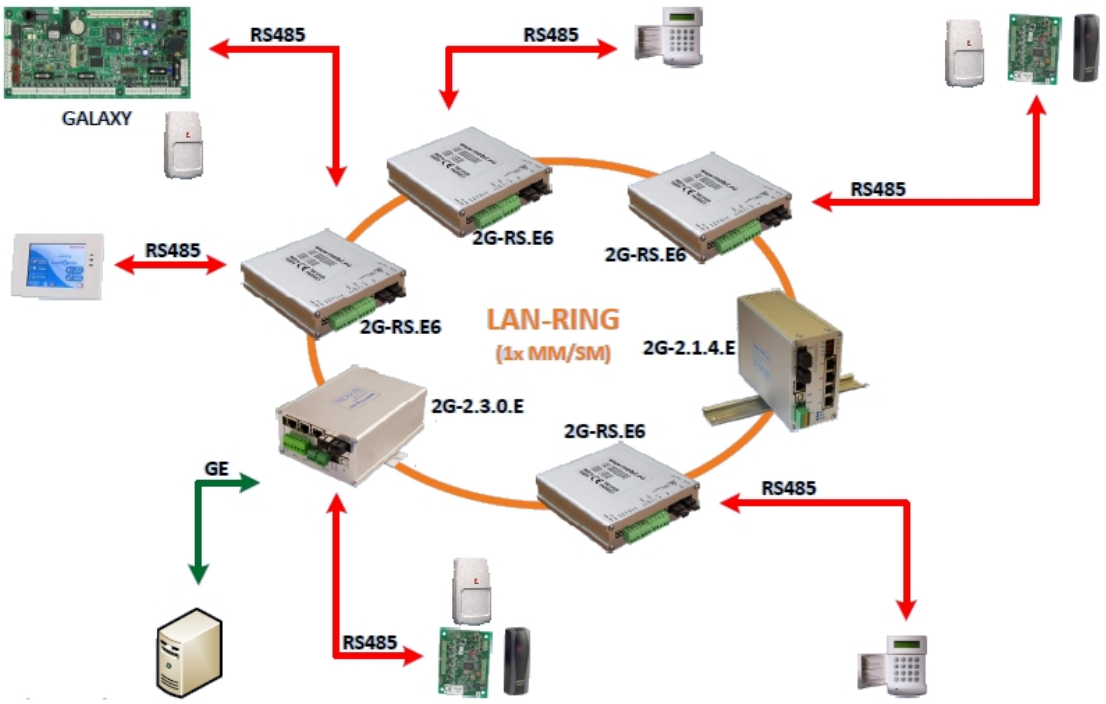
V následující tabulce jsou uvedené komponenty k rozšíření poplachového zabezpečovacího systému o přístupový systém.

Tab. 8. Použité prvky přístupového systému.

Zařízení	Název/Typ	Počet kusů
Řídící modul	Řídící modul C081/ pro dvě čtečky	8
Čtečka karet	Motorola Indala řada ASR-6xx	8
Identifikační zařízení	Bezkontaktní přívěšek GALMAX04	300

Řídící moduly C081, na které jsou připojené čtečky Indala, obsahují ovládací relé, pomocí kterého se ovládají elektromechanické zámky u obvodových dveří po celém objektu. Jednotlivé přístupové úrovně budou nastaveny přes zabezpečovací ústřednu, která bude také shromažďovat informace o pohybu zaměstnanců. Řídící modul obsahuje zdroj a rozšiřující koncentrátor na 8 zón.

Na níže uvedeném obrázku je znázorněno propojení PZTS a přístupového systému s využitím integračních prvků od firmy Metel, kde jednotlivé integrační komponenty budou popsány v další části zpracování návrhu systému.



Obr. 29. Příklad propojení PZTS a ACS do LAN-RING [43].

Výhodou propojení pomocí integračních modulů do kruhové topologie je zvýšení bezpečnosti přenosových tras. Porucha jedné části kruhu nemá žádný negativní vliv na funkčnost celého systému.

4.1.5.3 Perimetrický systém

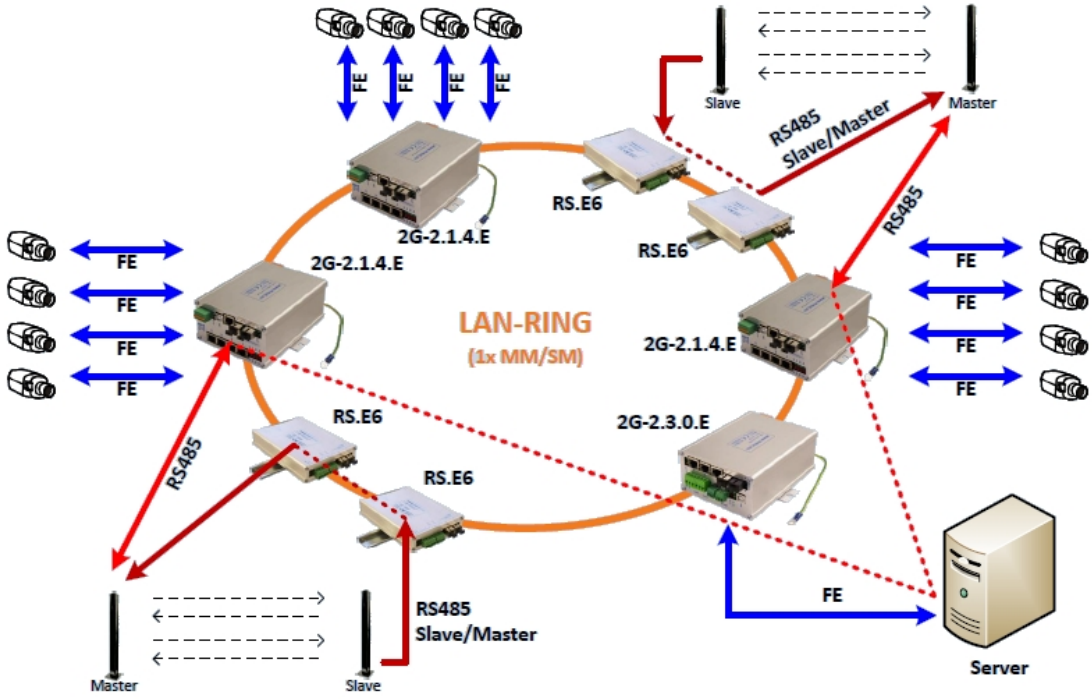
Efektivního zabezpečení docílíme instalováním perimetrického zabezpečovacího systému, který informuje o poplachové události dříve, než ji pachatel může začít vykonávat. Vzájemným propojení funkcí jednotlivých poplachových aplikací získáme takzvané předpoplachové informace, které jsou z hlediska reakce na danou situaci nejdůležitější.

Integrační moduly od firmy Metel mají vytvořené prostředí pro připojení perimetrických systémů ABSOLUTE SICURIT PIDS.

Tab. 9. Použité prvky pertimetrického systému.

Zařízení	Název/Typ	Počet kusů
Bariéra	Duální bariéra ABSOLUT/IMN200/2	2

Následující obrázek představuje zapojení duálních bariér pomocí switche RS.E6 do kruhové topologie. Propojené switche pomocí fast ethernet (FE) portu mohou mít připojeny kamerové systémy. Rozhraní pro připojení bariér do LAN-RING tvoří WDM multiplexory RS.E6.



Obr. 30. Příklad propojení perimetrického systému do LAN_RING [43].

Komunikace mezi bariérou probíhá pomocí MASTER/SLAVE, kdy jedno zařízení/proces přebírá jednosměrné řízení nad jinýma zařízeními.

4.1.5.4 Kamerový systém

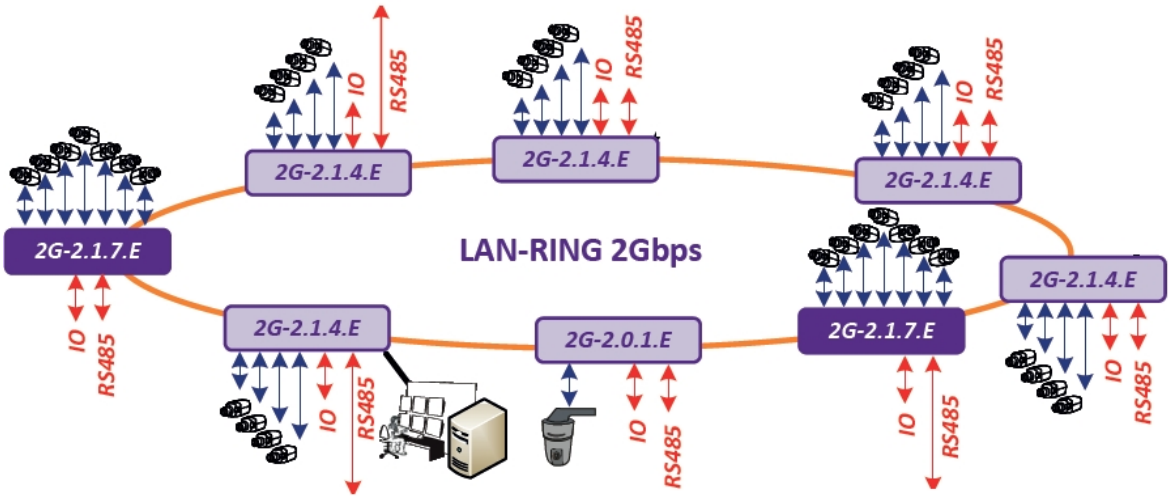
Použití kamerového systému v integrovaném poplachovém systému zpřehledňuje situaci ve střeženém objektu a jeho okolí. Pro snadnější zpracování informací z kamer je výhodné použít síťové IP kamery. Zde budou použité kamery od výrobce Axis. Kamerový systém bude sloužit k monitorování přístupových míst do jednotlivých budov objektu.

Použité komponenty kamerového systému jsou uvedeny v následující tabulce.

Tab. 10. Použité prvky kamerového systému.

Zařízení	Název/Typ	Počet kusů
IP kamera	Fixní / AXIS P1343-E	12
	Fixní / AXIS P1343	3
	PTZ / AXIS Q6032-E	6

Propojení jednotlivých kamer do kruhové topologie je realizováno pomocí průmyslových switche 2G s rychlou rekonfigurací do 30 ms, jsou odolnější vůči vnějším vlivům prostředí v místě nasazení.



Obr. 31. Příklad propojení kamerového systému do LAN_RING [43].

Switche jsou kromě ethernetových portů (optika/twist) osazeny dalšími porty jako jsou například RS485, RS422, RS232, digitální vstupy, relé výstupy, TTL vstupy/výstupy a audio vstupy/výstupy. To umožňuje propojit jedním optickým vláknem více různých systémů.

4.1.5.5 Integrující hardwarové prvky

Základním prvkem při integraci poplachových systému s využitím prvků informační technologie jsou **průmyslové switche**, **optické převodníky a media konvertory** vzájemně propojené na optické lince. V našem případě budeme využívat mnohavidové (MM - multimode) optické vlákno. V tomto návrhu IPS budou nejvíce využívány **PoE+ managed switche systému LAN-RING**. Na switche lze připojit jednotlivé kamery, ústředny PZTS, klávesnice, koncentrátory a PC (server).

Tab. 11. Použité integrační prvky LAN-RING systému.

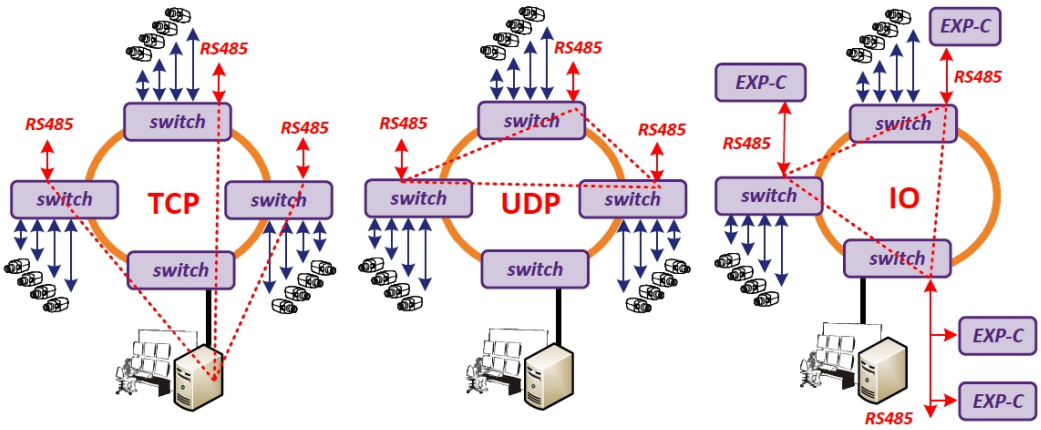
Zařízení	Název/Typ	Počet kusů
Managed - Switch	2G - 2.1.7. E	7
	2G – RS.E	4

Technické parametry PoE+ managed switch

Využívá kruhové topologie LAN-RING, která je vhodná zejména pro rozsáhlé zabezpečovací a automatizační systémy. Přepěťové ochrany na Fast Ethernetových portech switche zaručují spolehlivý provoz i při instalaci ve venkovním prostředí.

Obr. 32. PoE+ managed switch 2G-2.1.7.E [43].

Switche jsou osazeny **1x RS485** portem. Port může být nastaven ve třech základních režimech:



Obr. 33. Základní režimy nastavení switche [43].

Switche, které jsou připojeny do kruhové topologie, obsahují port RS485, který může být nastaven ve třech základních režimech uvedených na obrázku:

- TCP server – pro přímé propojení s aplikací na řídícím serveru,
- UDP režim – pro propojení 2 a více zařízení s požadavkem na externě nízkou latenci. Typická latence je kolem 3-4ms na 9,6kbps,
- IO (EXP-C) režim – pro připojení až 15 kusů I/O jednotek (EXP-C), například teplotní senzory [43].

Switche jsou osazeny **2x digitálními vstupy**, které jsou kompatibilní s vyváženými smyčkami všech alarmových systémů. Stav vstupů lze odesílat SNMP protokolem do integračního software C4. Stav vstupů jde také přemapovat na relé na dalších switchích nebo I/O modulech. Vše je možné nastavit lokálně přes USB port nebo vzdáleně po LAN softwarem SIMULand.

Switch obsahuje **1x programovatelné relé** výstup, který může být například aktivován:

- výpadkem spojení po LAN nebo RS485, přerušením optického kruhu,
- sepnutím/rozepnutím jednoho nebo více vstupů na dalších switchích a I/O modulech,
- funkcí IPwatchdog která automaticky restartuje „zablokována“ zařízení,
- SNMP protokolem s integračního software C4.

Switch obsahuje **2x** Multimode (**MM**) / Singlemode (**SM**) univerzální **optické porty** použitelné v rozsahu od 8/125µm do 62,5/125µm. Optické porty mají integrovanou technologii vlnového multiplexu (WDM). Optický kruh/spoj je tak tvořen pouze jedním MM vláknem, které je vhodnější na kratší vzdálenosti.

Switch je osazen **1x Gigabit ethernet** portem podporující standardy 10BASE-T, 100BASE-TX včetně funkcí: Auto-negotiation, Auto MDI/MDI-X a Power-down. Dále obsahuje **7x Fast Ethernet** port s podporou PoE+ podporující stejné standardy jako gigabit etherne. Porty také podporují napájení koncových zařízení po Cat-5e kabelu dle norem IEEE 802.3-af / IEEE 802.3at, kde maximálně máme 25,5W na port.

Switch obsahuje **1xPoE výstup** s podporou PoE+, **2x** nezávislé **vstupy napájení**. Switche mají na Fast Ethernetových portech integrovaný **IP Watchdog**, který v případě poruchy může resetovat PoE napájení, aktivovat relé výstup nebo odeslat SNMP trap [43].

Podpora:

- SNMP – protokol pro sběr dat a řízení přes LAN,
- SMTP – protokol pro odesílání emailů,

- SNTP – protokol pro centrální synchronizaci času,
- IGMP – protokol pro management multicastových skupin,
- UPNP – protokol pro detekci zařízení připojených k LAN (switche pouze podporují transfer UPNP paketů).

Standardy a protokoly:

- **IEEE 802.3i** - 10BASE-T 10 Mbit/s (1.25 MB/s) over twisted pair IEEE 802.3u for 100BaseT(X), 100BaseFX,
- **IEEE 802.3u** - 100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet 100 Mbit/s (12.5 MB/s) w/autonegotiation,
- **IEEE 802.3ab** - 1000BASE-T Gbit/s Ethernet /twisted pair 1 Gbit/s (125 MB/s),
- **IEEE 802.3ac** - Max. 1522 byte ("Q-tag"),
- **IEEE 802.3af -** Power over Ethernet (15.4 W),
- **IEEE 802.3at** - Power over Ethernet enhancements (25.5 W),
- **IEEE 802.1p -** Class of Service,
- **IEEE 802.3x** - Flow Control,
- **IEEE 802.1q -** VLAN Tagging,
- **Modbus/TCP -** RS485 port,
- **DHCP Client -** Protocol for automatic IP configuration,
- **Management** - USB – lokální heslem chráněný management přes USB A/B kabel SW SIMULand - šifrovaný management přes LAN [43].

Pro připojení perimetrického systému do kruhové topologie LAN-RING použijeme **Managed switche 2G.RS.E.** Dále lze tento switch využít na připojení poplachových ústředen, klávesnic, koncentrátorů do kruhové topologie. Perimetrické bariéry a ústředny jsou propojeny se switchem přes RS485/RS232.

Obr. 34. Managed switch 2G.RS.E [43].

Technické parametry Managed switche 2G.RS.E

Vychází ze základních parametrů PoE+ managed switche, jen s tím rozdílem že není osazen vstupy PoE. Základní funkcí switche je připojení poplachových systémů přes RS485/RS232 na kruhovou topologii LAN-RING. Obsahuje následující parametry:

- MM/SM vlákno univerzál s WDM,
- 1/2x optické porty,
- 2x digitální vstup,
- 1x programovatelné relé,
- RS485/RS232 port s podporou:
    - APOLLO, ASSET, ATS, CAIS, DOMINUS, **GALAXY**, HUB-PRO, PERIDECT, ROGER, SATEL-ACCO, **SICURIT-ABSOLUTE**, STATOIN-ONE, Modbus RTU/ASCII,
- 2 vstupy napájení,
- přepěťová ochrana,
- provozní teplota -40 ℃ do + 70 ℃,
- podpora SNMP,
- TCP server,
- certifikace s PZTS (DOMINUS, GALAXY) [43].

4.1.6 Konfigurace systému

Integrovaný systém musí být navržen tak, aby splňoval všechny požadavky, které byly na začátku navrženy. Systém bude naprogramován na provozní režimy, které budou přizpůsobeny pracovnímu režimu v objektu. První režim je **denní směna**, při které bude většina zaměstnanců v práci. Druhy režim je **noční směna**, při které bude v provozu výrobní hala a administrativní budova bude ve stavu střežení (ARM), mimo šaten pro zaměstnance. Třetí režim je **doba bez provozu**, tím to se rozumí státní svátky, nevynucená odstávka výroby a další režimy, při kterých budou obě budovy v režimu střežení.

4.1.6.1 Hlavní funkce systému

Funkce systému budou soustředěny na jednotlivé režimy IPS, které mohou nastat v důsledku provozu výroby. Hlavní funkce u **denní směny** je zamezení neoprávněného pohybu osob po objektu. Každý zaměstnanec bude mít identifikační předmět ve stylu

přístupové karty, pomocí kterých si bude otvírat příslušné dveře. Každý vchod do výrobní i administrativní budovy bude monitorován kamerovým systém, který zpřehlední situaci v objektu. Kamerový systém napomáhá odhalit neoprávněnou manipulaci s materiálem, pohybu osob a vzniklým problémem při identifikaci uživatele.

Funkce, které budou plnit své poslání v režimu **noční směna**, budou vycházet z denního provozu jen s tím rozdílem, že administrativní budova bude částečně ve stavu střežení. Šatna pro zaměstnance je v přízemí administrativní budovy, proto systém bude nastaven tak, aby při identifikaci uživatele u vstupních dveří se odstřežila (DISARM) přístupová chodba a šatna pro zaměstnance. Po odchodu pracovníka z administrativní budovy se automaticky zapne okruh poplachových detektorů, které byly odkódovány.

Funkce při režimu **doba bez provozu** budou vycházet z celkového zastřežení objektu. Příjezdové cesty budou střeženy pomocí perimetrického systému. Při jakémkoliv narušení chráněného objektu bude informována zásahová skupina bezpečnostní agentury.

Hlavní funkce sytému jsou soustředěny na bezpečnostní přínosy:

- zvýšení přehledu o situaci v objektu,
- dostupnost potřebných informací (text, obraz, vizualizace),
- podpora rychlejší reakce na danou situaci,
- podpora řešení krizových situací.

Další hlavní funkce jsou z hlediska ekonomického přínosu:

- snížení energetické závislosti objektu (osvětlení, vytápění),
- snížení nákladů na zabezpečení ochrany majetku,
- snížení nákladů na pořízení IPS vzhledem k instalaci samostatných systémů.

4.1.6.2 Informace pro ovládání systému

Ovládání systému bude rozděleno na více přístupových úrovní. Od ovládacího rozhraní pomocí **klávesnice** PZTS, kde budou mít zaměstnanci přidělené funkce zapnout/vypnout poplachový systém. Dále ovládání bude probíhat pomocí **software C4**, který bude nainstalován v místě obsluhy vrátného v administrativní budově. Nastavení switche bude probíhat pomocí software SIMULand, který bude sloužit pro pracovníci montážní firmy. Ovládání vstupních dveří do objektu probíhá pomocí **přístupových karet** do jednotlivých úseků.

Na vrátnici v administrativní budově při denní směně je obsluha, která má na starost kontrolu pohybu zaměstnanců po celém objektu pomocí vizualizačního softwaru. Dále jako první příchozí do administrativní budovy musí odstřežit zabezpečovací systém. Vrátný jako poslední odcházející z administrativní budovy musí zapnout systém do stavu střežení, ale jen zabezpečovací systém administrativní budovy.

Ovládání kamerového systému probíhá na vrátnici proškoleným pracovníkem. Pracovník, zde může sledovat jednotlivé obrazy z fixních kamer a PTZ kamery si může pomocí ovládacího panelu nastavit na danou pozici.

4.1.6.3 Informace o programování systému

Integrovaný poplachový systém bude rozdělen na podsystémy: administrativní budova a výrobní hala. Programováním poplachových systémů vycházíme ze vzájemného propojení funkcí jednotlivých aplikací. Základem bude naprogramování PZTS s přístupovým systémem a kamerovým systémem.

Vchody do **administrativní budovy** budou ovládány pomocí čtečky karet, která po přiložení identifikačního předmětu aktivuje elektromechanický zámek umístěný ve dveřích a umožní vstup do budovy. Po přiložení identifikačního čipu, bude následovat otočení PTZ kamery na nastavenou pozici monitorující daný vchod do budovy. Hlavní vchod do administrativní budovy je monitorován fixní kamerou. V pracovním režimu **noční směny** bude administrativní budova zastřežena. Určité zóny PZTS, které spadají pod chodbu a šatny pro zaměstnance se odkódují po přiložení identifikační čipu u příslušného vchodu do budovy. Pohybový detektor a magnetický kontakt u hlavního vchodu do budovy bude mít časové zpoždění pro případné odkódování zabezpečovacího systému. První **klávesnice CP041** pro ovládání PZTS bude umístěna na chodbě u hlavního vchodu. Druhá **klávesnice MK7** bude umístěna na vrátnici, kde bude probíhat ovládání celého IPS. Každá místnost v administrativní budově bude osazena pohybovými **detektory IS2560T** a okna magnetickými kontakty, které budou nastavený na typ okamžitého vyhlášení poplachu. Kamerový systém administrativní budovy tvoří dvě venkovní **PTZ kamery**, které monitorují vchod a přilehlé okolí budovy. Obsluha může zareagovat na vzniklou situaci natočením kamery, pomocí ovládacího panelu. Fixní kamery trvale monitoruji všechny vchody do budovy a vstupní chodby v budově.

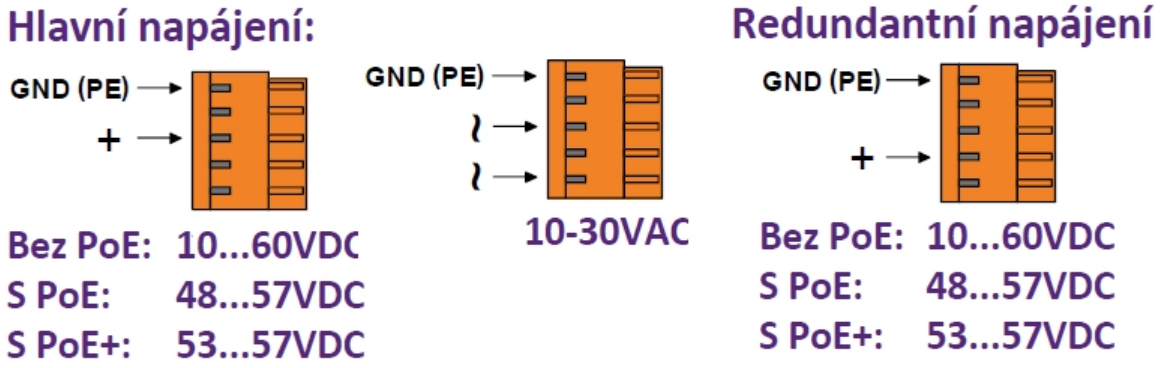
Provoz ve **výrobní hale** je na jednotlivých úsecích celodenní, tím pádem musí být integrovaný systém naprogramovaný na tuto situaci. Každý vchod do výrobní haly je osazen čtečkou karet, která aktivuje elektromechanický zámek umístěný ve dveřích. U všech vchodu je uvnitř haly pohybový detektor **IS2560T** a na vstupních dveřích magnetický kontakt. Vjezdové vrata, jsou osazeny vratovým magnetickým kontaktem, který je střeží před neoprávněným otevřením. Jak u vchodových dveří, tak u vjezdových vrat bude nastavená časová prodleva, kdy po jejím překročení obsluha bude informována o delším otevření než v normální situaci. Otočné **PTZ** kamery se nastaví na předem nastavenou pozici snímající vjezdové vrata či vchodové dveře. Uvnitř haly jsou rozmístěny **fixní** kamery, které monitorují jednotlivé výrobní provozy. V režimu střežení (ARM) jsou všechny magnetické kontakty a pohybové detektory nastaveny na okamžité vyhlášení poplachu.

Perimetrický systém je v aktivaci jen v případě celkového zastřežení objektu. Perimetrické bariéry jsou nastaveny na příjezdové cesty a přístupové místa k objektu.

Důležitým prvkem správného chodu integrovaného poplachového systému je naprogramování **switche** zapojených do kruhové topologie LANG-RING.

Instalaci a nastavení PoE+ managed switche budeme provádět následovně:

- **Připojením napájení** 10 – 60 VDC nebo 10 – 30 VAC uvedeno níže na obrázku. Napájení je signalizováno rozsvícením žluté LED. Přepěťové ochrany jsou uzemněny přes zelenožlutý vodič, který spojíme se zemí vodiče s minimálním průřezem 1,5mm^2.



Obr. 35. Napájení PoE+ managed switch [43].

- **Připojením optického vlákna** zakončeného konektorem SC, broušení typu PC. Z důvodu vlnového multiplexu je nutné zapojovat optické porty do kříže, to znamená port P10 do portu P11 atd. Před uzavřením optického kruhu musí být jeden switch nastaven jako Master.

1000Base-BX je verzí Fast Ethernetu, která využívá jednovidové optické vlákno a pro vysílání a přijímání se používají dvě vlnové délky. Definice dle IEEE802.3ah je uvedena v následující tabulce:

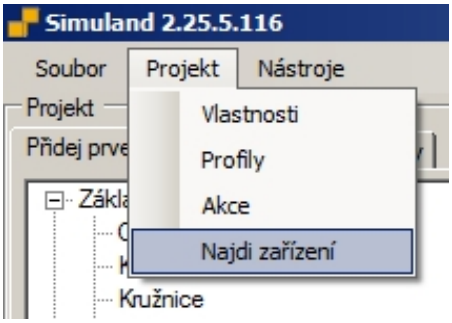
Tab. 12. Definice 1000BASE-BX [43].

----------	Požadavek normy	PoE+managed switch
Počet vláken	1	1
Typ vlákna	singlemode	singlemode
Dosah	10 km	20 km
Upstream	1310 nm	1310 nm
Downstream	1550 nm	1550 nm
Maximální útlum	5,5/6 dB	14 dB

- **Připojením signálového vedení:**
  - **RS485** – připojením sběrnice A+ a B-, A+ má bez dat kladnější hodnotu,
  - **USB –** konektor pro připojení USB A-B kabelu pro ovládání management pře software SIMULand,
  - **RELÉ –** v alarmovém stavu je spojeno COM a N.O. Alarmovým stavem je výpadek napájení, ztráta komunikace a přerušení optického vlákna,
  - **IN/OUT –** digitální vstupy aktivujeme sepnutím ke GND nebo úrovní TTL (0-0,3V „log 0“ a 2,7-5V „log 1“). TTL výstupy lze mapovat v managementu switche [43].

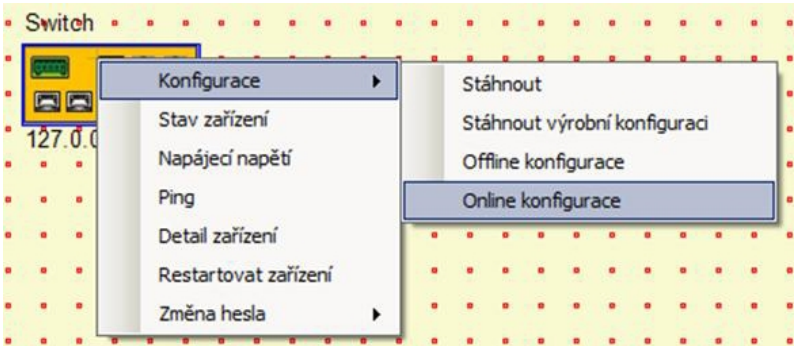
Pro **konfiguraci PoE+ managed switche** budeme postupovat následovně.

- Stáhneme a nainstalujeme softwarovou aplikaci **SIMULand,** kterou spustíme.
- V menu „**Projekt/Najdi zařízení**“ naskenujeme dostupná zařízení a vložíme je přetažením na plochu. IP adresa síťové karty musí být nastavena ve stejném rozsahu IP adres, jako je IP adresa switche.



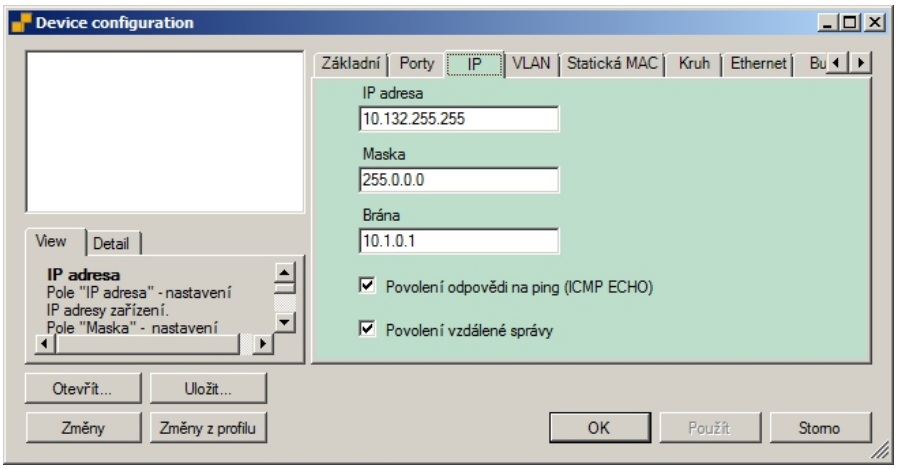
Obr. 36. Skenování zařízení [43].

- Vybereme kurzorem myši zařízení, kliknutím levého a poté pravého tlačítka myši. Zvolíme v menu „ **Konfigurace/Online konfigurace**“ a vložíme požadované heslo na přihlášení.



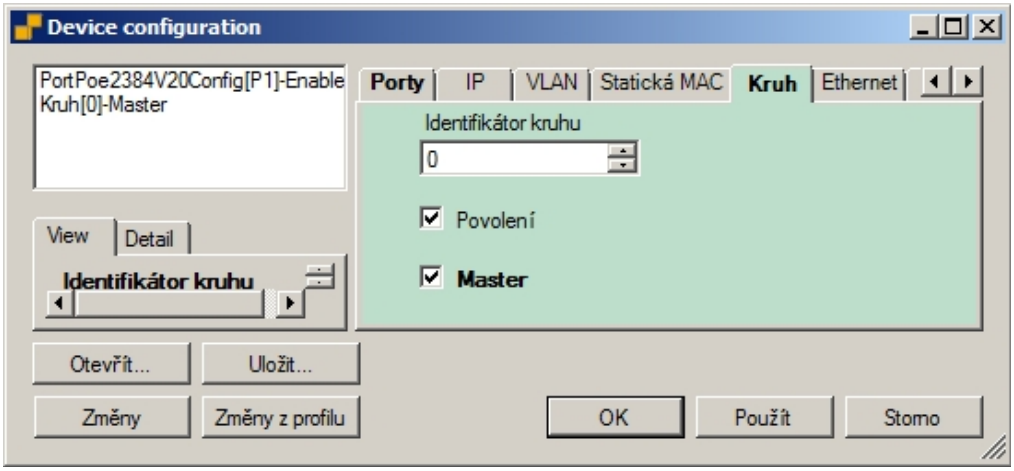
Obr. 37. Konfigurace zařízení [43].

- Základní nastavení v menu „**IP**“ zvolíme – nastavení IP adresy, masky a brány. „**Povolení odpovědi na ping**“ – Povolit/zakázat switchi reagovat na příkaz ping. „**Povolení vzdálené správy**“ - zatrhnutím položky se budeme moci do switche připojit pouze přes USB.



Obr. 38. IP konfigurace [43].

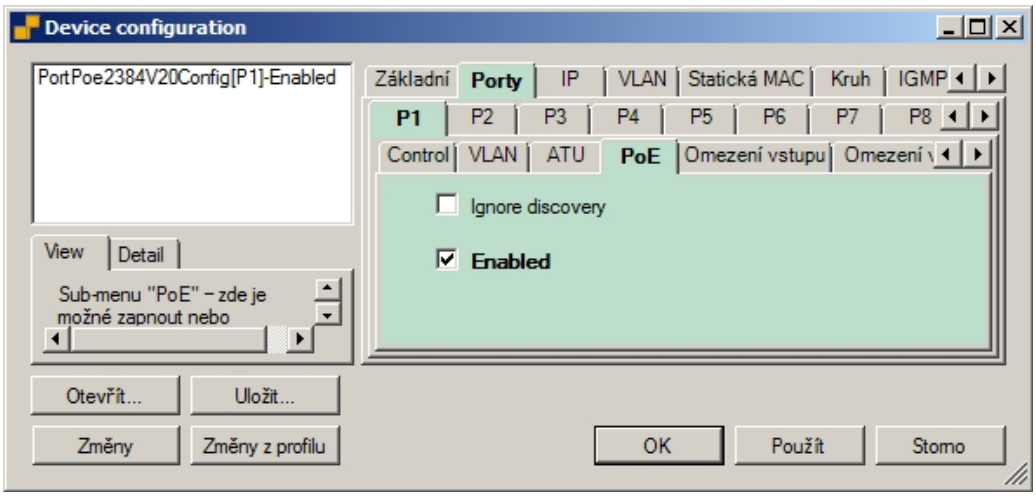
- Před uzavřením optického kruhu musíme v menu „**Kruh**“ nastavit vždy jeden switch jako „**Master**“. Pro použití více optických kruhů nastavte každému kruhu jiný „**Identifikátor kruhu**“.



Obr. 39. Nastavení MASTER v kruhové topologii [43].

Aktivace PoE+ na Fast Ethernet FE portech

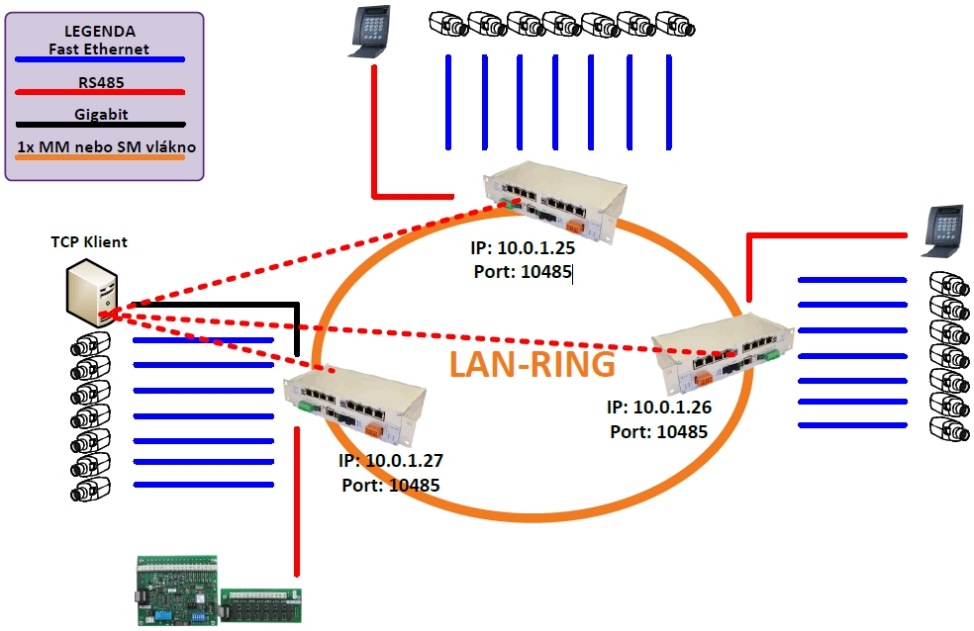
V hlavním menu „**Porty**“ vybereme požadované FE porty („**P1 – P7**“), na kterých aktivujeme PoE+ napájení. Port „**P8**“ slouží pouze k napájení PoE+ a nepřenáší žádná data. Zatrhnutím položky „**Enabled**“ povolíme napájení PoE na portu. Položka „**Ignore discovery**“ zapne trvale napájení na PoE bez ohledu mna detekci a klasifikaci koncového PoE zařízení [43].



Obr. 40. Aktivace PoE+ na Fast Ethernet potrech [43].

Natavení **TCP** protokol (Transmission Control Protokol) na přenos dat mezi prvky umístěné v jedné síti. Výhoda u TCP protokolu je **spolehlivost přenášených dat**. Protokol využívá potvrzení přijatých dat, opětovné posílání a překročení časového limitu. Další výhoda je zachování pořadí přijatých dat na switch.

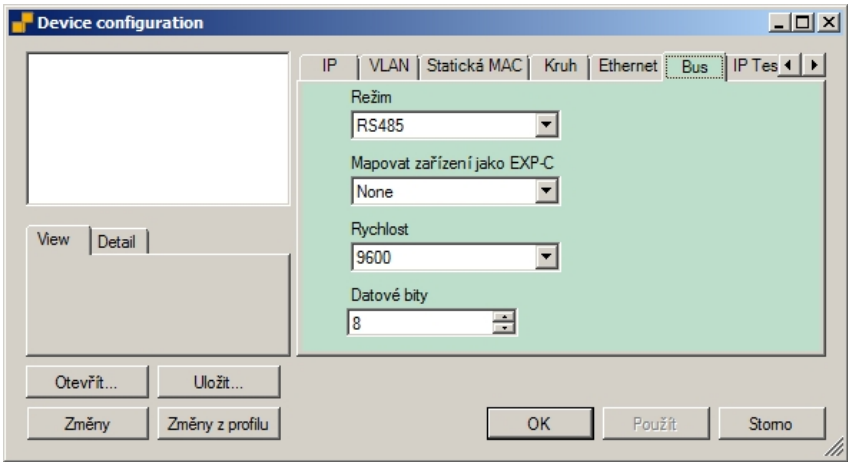
Nastavení přenosu RS485 v TCP režimu



Obr. 41. Nastavení přenosu v TCP režimu [43].

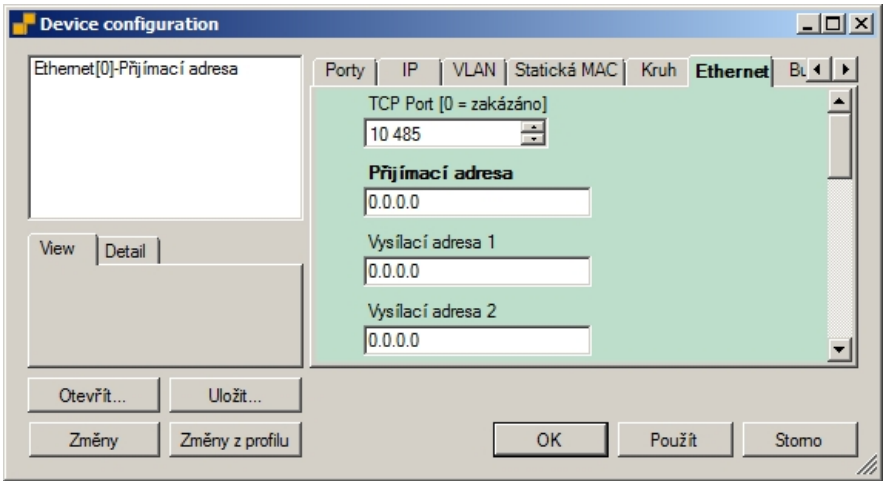
Nastavení se skládá z následujících kroků.

- V menu „**Bus/Mode**“ vybereme požadovaný systém. Pokud není v menu uveden, zvolíme volbu „**RS485**“ a nastavíme „**Rychlost**“ a „**Datové bity**“. Pokud je název systému v seznamu uveden, nejsou již další nastavení v menu „**Bus**“ potřebné. Switch si je nastaví automaticky.



Obr. 42. Nastavení RS485 [43].

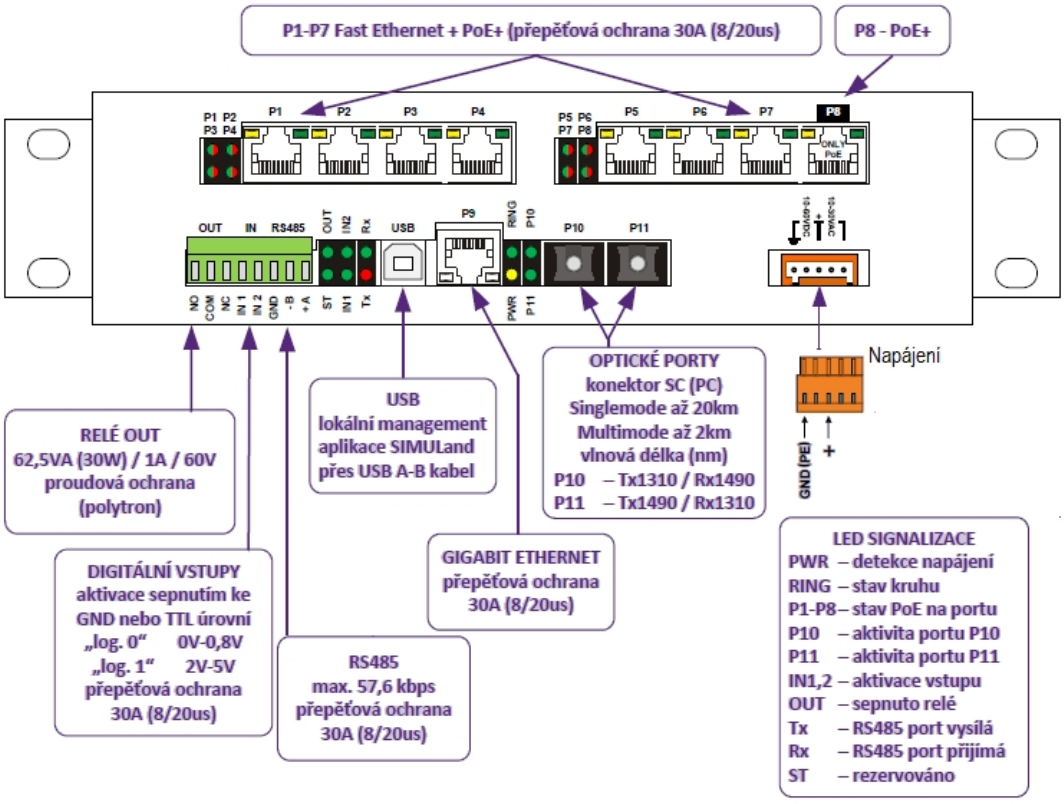
- V menu „**Ethernet/TCP Port**“ nastavte číslo portu, na které naváže TCP klient spojení.



Obr. 43. Nastavení TCP portu [43].

- Nakonfigurujeme TCP klienta v PC s nainstalovaným integračním softwarem.

Následující obrázek představuje přední panel **PoE+ Managed Switch,** pro lepší orientaci je panel osazen LED signalizací, která zobrazuje právě probíhající stavy na switchi.



Obr. 44. Panel PoE+ Managed Switch [43].

4.1.6.4 Rozmístění použitých prvků

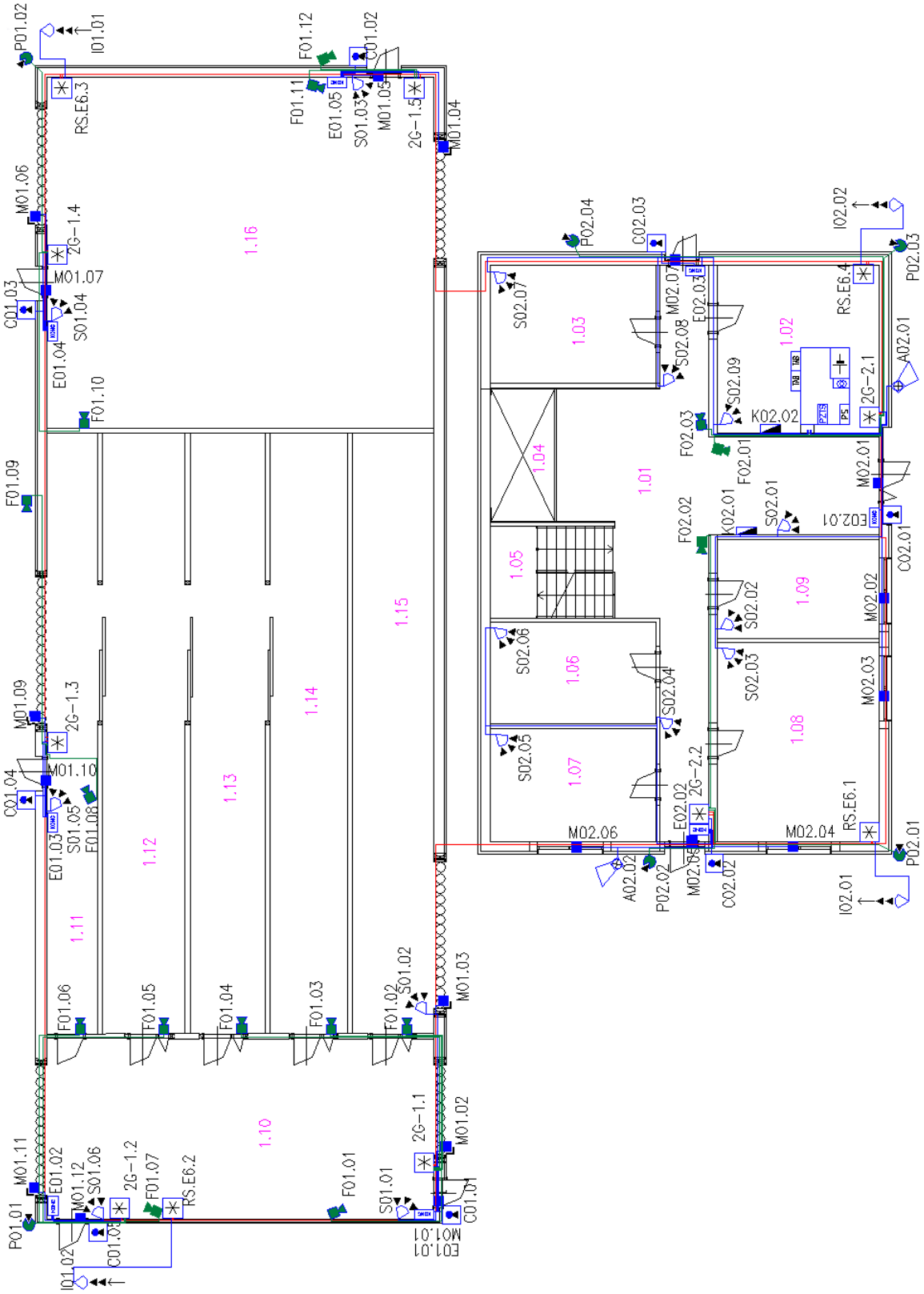
Jednotlivé komponenty integrovaného poplachového systému budou rozmístěny dle následujících schémat vystihující půdorys průmyslového objektu. Zařízení jsou označeny podle druhu, do jakého podsystému spadají a pořadové číslo.

- S0x.0x – pohybové detektory,
- M0x.0x – magnetické kontakty,
- C0x.0x – čtečka přístupových karet,
- A0x.0x – akustická signalizace,
- E0x.0x – koncentrátor,
- 2G-x.x - PoE+ managed switch,
- RS.E6.x - Managed switch,
- F0x.0x – fixní kamera,
- P0x0x – PTZ kamera.

Následující tabulka zobrazuje schematické značky, které jsou posléze použity u znázornění umístěných prvků integrovaného poplachového systému.

	Magnetický kontakt dveře + okna		Čtečka karet
	Magnetický kontakt vrata		Klávesnice PZTS
	PTZ kamera	KONC	Expander
	Fixní kamera	TAB	Tablo
	Pohybový detektor		Trafo
	Průmyslový switch	PZTS	Ústředna PZTS
	Akustická signalizace	PS	Napájecí zdroj
	Infrazávora přijímač		Záložní akumulátor
	Infrazávora vysílač		

Obr. 45. Schámatické značky.

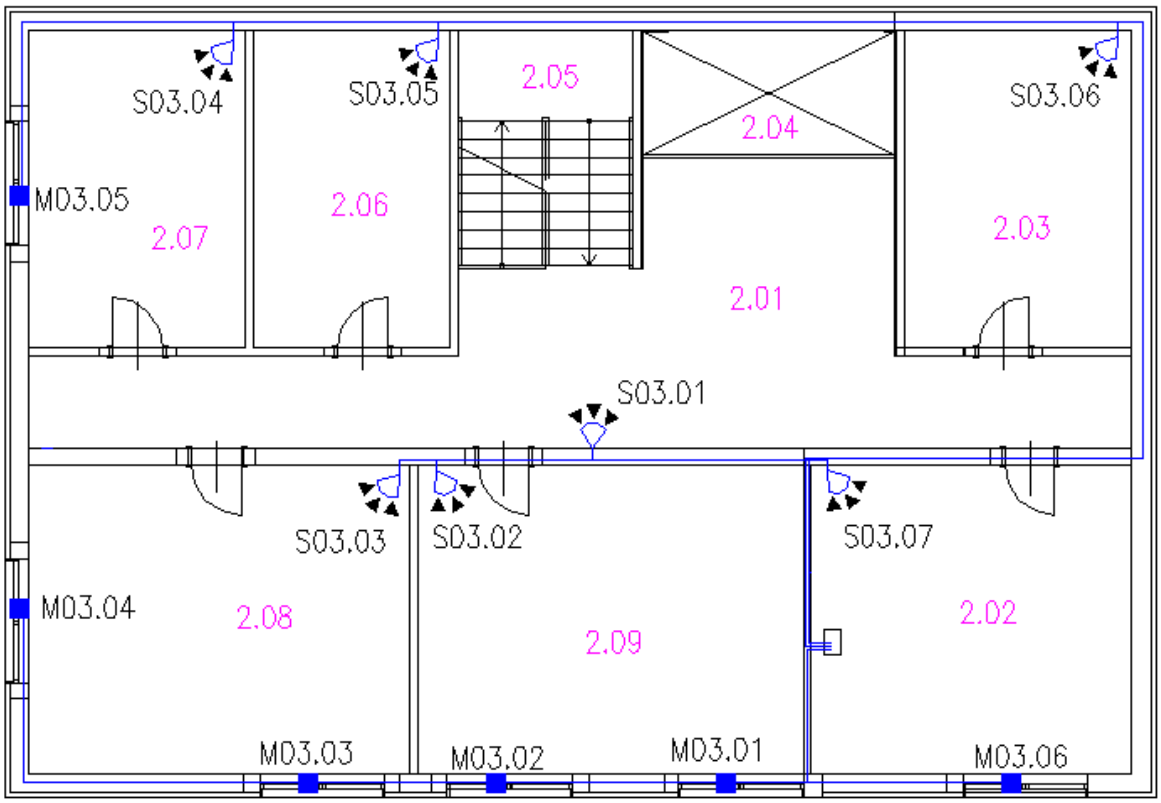


Obr. 46. Rozmístění prvků: administrativní budova 1.NP a výrobní hala.

Značení kabeláže je rozděleno barevně dle použitého typu.

- Červená – optické MM vlákno.
- Zelená – Fast Ethernet (UTP kabel).
- Modrá – RS 485 (kroucená dvojlinka).

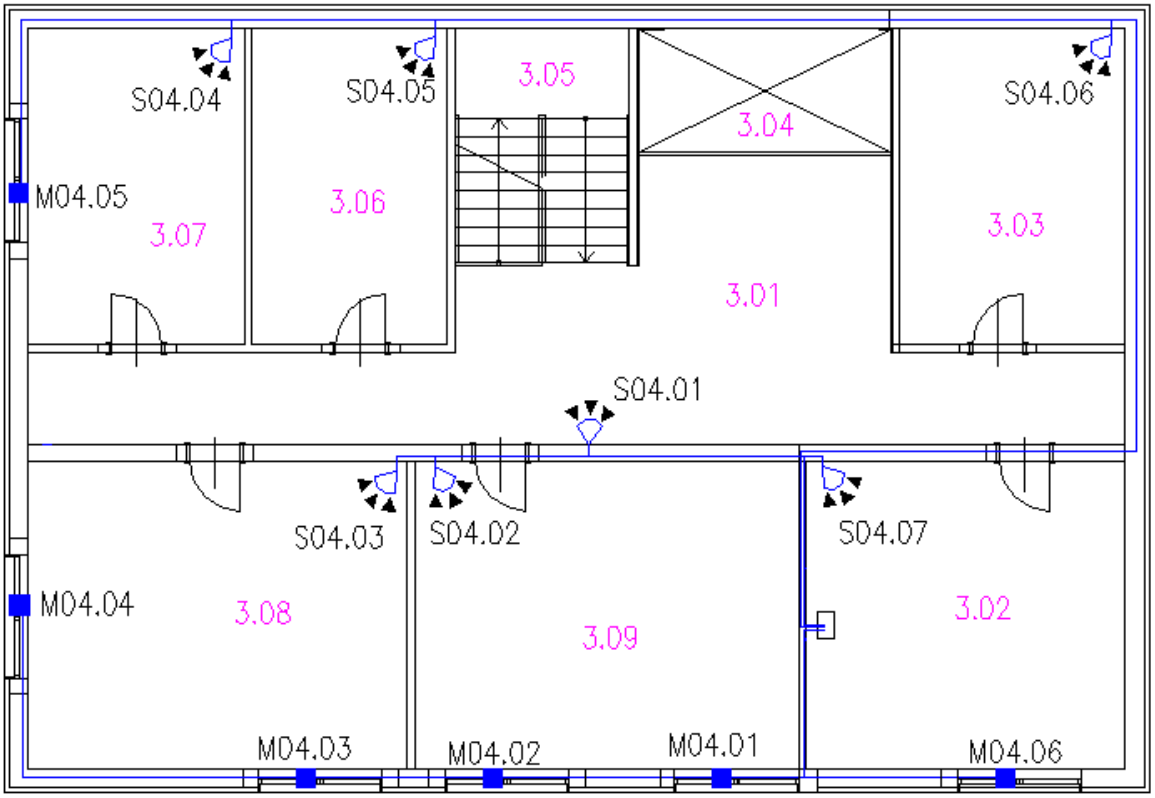
Následující obrázek představuje umístění prvků poplachového zabezpečovacího a tísňového systému v 1. patře administrativní budovy.



Obr. 47. Rozmístění prvků: administrativní budova 2.NP.

Prvky v 1. a 2. patře administrativní budovy jsou napojené pomocí kroucené dvojlinky přímo na ústřednu PZTS, která je připojena na optickou linku pomocí průmyslového switche.

Následující obrázek představuje umístění prvků poplachového zabezpečovacího a tísňového systému v 2. patře administrativní budovy.



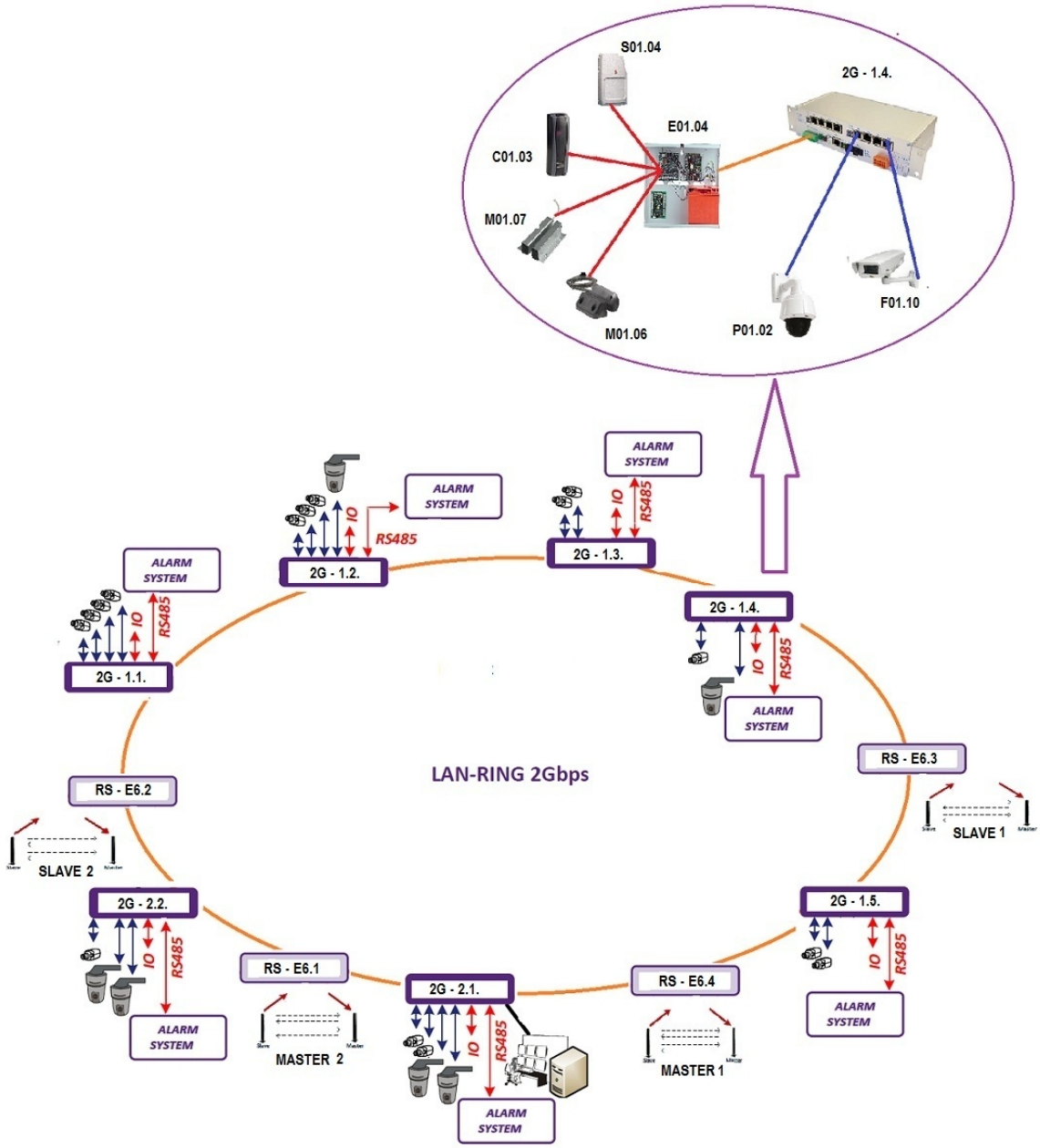
Obr. 48. Rozmístění prvků: administrativní budova 3.NP.

V následující tabulce je rozpis jednotlivých místností v administrativní budově a pracovních úseků ve výrobní hale.

Tab. 13. Rozpis místností.

Administrativní budova 1.NP		**Administrativní budova 2.NP**	
1.01	Chodba 1.NP	2.01	Chodba 2.NP
1.02	Vrátnice	2.02	Kancelář č.1
1.03	Úklid	2.03	Archiv
1.04	Výtahová šachta	2.04	Výtahová šachta
1.05	Schodiště	2.05	Schodiště
1.06	Toalety	2.06	Toalety
1.07	Sprchy	2.07	Kancelář č.2
1.08	Šatna	2.08	Kancelář č.3
1.09	Technická místnost	2.09	Kancelář č.4
Výrobní hala		**Administrativní budova 3.NP**	
1.10	Nákladní prostor	3.01	Chodba 3.NP
1.11	Výrobní úsek č.1	3.02	Kancelář č.1
1.12	Výrobní úsek č.2	3.03	Archiv
1.13	Výrobní úsek č.3	3.04	Výtahová šachta
1.14	Výrobní úsek č.4	3.05	Schodiště
1.15	Výrobní úsek č.5	3.06	Toalety
1.16	Výrobní úsek č.6	3.07	Kancelář č.2
		3.08	Kancelář č.3
		3.09	Kancelář č.4

Prvky, které jsou zakreslené v půdorysu objektu, jsou zapojeny dle následujícího blokového schématu v kruhovou topologii LAN-RING 2Gbps. Základním propojovacím prvkem kruhové topologie je optické MM vlákno, na které jsou připojeny průmyslové switche. Switche zpracovávají vstupní signály z připojených zařízení, které pak dále odesílají do MASTER switch, který vyhodnocuje danou situaci na optickém kruhu.



Obr. 49. Schéma integrovaného poplachového systému.

Integrovaný poplachový systému bude obsahovat 7 x PoE + Managed switch a 4 x Managed switch RS–E.6. Rychlost optického kruhu je 2Gbps (Giga bit per sekond) jednotka přenosové rychlosti udává, klik bitů informace je možné přenést za jednu sekundu. Maximální datový tok v kruhu ≤ 800 Mbps.

4.1.7 Hlášení poplachu a poruchy

Objekt bude napojený na **dohledové poplachové přijímací centrum** bezpečnostní agentury, která v případě obdržení zprávy o narušení střeženého místa vyjíždí **zásahová jednotka**, která na místě provede zásah. Poplachová zpráva může přijít během noční směny, kdy je zakódována administrativní budova, nebo dále při celkovém zastřežení objektu. Přenos bude realizován pomocí **radiového spojení**. Zásahová skupina může celou situaci v objektu sledovat vzdáleně pomocí kamerového systému.

Na místě, kde je přes **denní směnu** proškolený pracovník, bude signalizace o narušení objektu realizována pomocí **vizualizačního softwaru**, který je nainstalovány na vrátnici na PC. Stanovení priorit vyhlášení poplachu a poruchy v systému:

- priorita 1 – poplachové signály (ochrana života, požár, napadení),
- priorita 2 – poplachové signály (ochrana majetku, nedovolené vniknutí),
- priorita 3 – poplachové signály z ostatních poplachových aplikací,
- priorita 4 – poruchové signály (ochrana života a majetku),
- priority 5 – poruchové signály z ostatních poplachových aplikací,
- priority 6 – informace z nepoplachových aplikací.

Na plášti administrativní budovy jsou instalovány dvě **venkovní sirény** se stroboskopem, které jsou v aktivaci při narušení zastřežené zóny.

4.1.8 Legislativa

Při realizaci integrovaného poplachového systému se musíme řídit stanovisky jednotlivých právních předpisů. Následující právní předpisy se vztahují na IPS.

- **Zákon č. 22/1997 Sb**., o technických požadavcích na výrobky,
- **Nařízení vlády č. 17/ 2003 Sb**., kterým se stanoví technické požadavky na elektrická zařízení nízkého napětí,

- **Nařízení vlády č. 616/2006 Sb**., o technických požadavcích na výrobky z hlediska jejich elektromagnetické kompatibility.
- **Nařízení vlády č. 426/2000 Sb**., kterým se stanoví technické požadavky na radiová a na telekomunikační koncová zařízení.
- **Vyhláška č. 50/1978 Sb.,** Českého úřadu bezpečnosti práce a Českého báňského úřadu o odborné způsobilosti v elektrotechnice.

4.1.9 Normy

Jednotlivé technické požadavky na IPS jsou uvedeny v příslušných normách pro každou poplachovou aplikaci. Tyto řady norem budou udávat požadavky na IPS:

- **ČSN EN 50 130** – Poplachové systémy – Všeobecné požadavky,
- **ČSN EN 50 131** – Poplachové systémy – Poplachové zabezpečovací a tísňové systémy,
- **ČSN EN 50 132** – Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích,
- **ČSN EN 50 133** – Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích,
- **ČSN EN 50 136** – Poplachové systémy – Poplachové přenosové systémy a zařízení,
- **ČSN CLC/TS 50 398** – Poplachové systémy – Kombinované a integrované systémy - všeobecné požadavky.

4.1.10 Certifikace

Certifikace LAN-RING dle ČSN EN 50131-1.

- **Monitorování**: detekce maximální povolené nedostupnosti propojení.

Tab. 14. Detekce monitorování.

1. stupeň	2. stupeň	3. stupeň	4. stupeň
100 s	100 s	100 s	10 s

Skutečnost v LAN-RING detekce v **milisekundách** / oprava spojení do **30ms**.

- **Ověřování**: periodická komunikace (intervaly)

Tab. 15. Ověřování komunikace.

1. stupeň	2. stupeň	3. stupeň	4. stupeň
240 min	120 min	100 s	2 s

Periodické ověřování v LAN-RING **probíhá každé 2s**.

- **Bezpečnost komunikace**
  - Zpracování signálu vniknutí a sabotáže >400ms.
  - Zpracování signálu poruch trvající > 10s.
  - Signály o vniknutí, sabotáže a poruchy musí být vyhlášeny do 10s.
  - Skutečnost u LAN-RING je **detekce v milisekundách** a **oprava spojení do 30ms .**
- **Pravidla správné instalace LAN-RING**
  - Převodníky jsou zapojeny do kruhu.
  - Relé výstupy pro detekci poruchy, sabotáže jsou zapojeny do PZTS.
  - Převodníky jsou nainstalovány v krytech s detekcí vniknutí.
  - Převodníky jsou napájeny z napájecího zdroje PZTS [43].

4.1.11 Zásah

V režimu **denní směny** bude zásah prováděn proškoleným pracovníkem, který bude informovaný pomocí vizualizačního softwaru. Bude se většinou jednat o dohlížení na dodržování přístupových úrovní zaměstnanci.

V režimu **noční směny** budou poplachové signály informovat pomocí radiového přenosu výjezdovou skupinu bezpečností agentury, která provede zásah na místě.

4.1.12 Údržba

O údržbu integrovaného poplachového systému se bude starat montážní firma. Bude se jednat o funkční zkoušky systému, které se budou provádět v intervalu 1x ročně.

4.1.13 Opravy

Potřebné opravy integrovaného poplachového systému bude provádět montážní firma s podporou dodavatelských společností, převážně se bude jednat o technickou podporu společnosti METEL s.r.o.

4.2 Systém LAN-RING

Při projektování průmyslových switche od firmy METEL se vychází ze dvou základních topologických zapojení, které jsou LAN-BUS a LAN-RING.

Topologie **LAN-BUS** používá jedno MM nebo SM vlákno, na kterých jsou zapojeny do série switche, čím se vytvoří optická sběrnice. Switche od firmy METEL jsou kompatibilní dle standartu 100BASE-BX a s topologii LAN-RING.

Topologie **LAN-RING** používá pro spojení switchů jedno MM nebo SM optické vlákno. Switche jsou většinou zapojeny do kruhu, ale uzavření není podmínkou. Switche jsou kompatibilní dle standartu 100BASE-BX a 1000BASE-BX. Výhody u LAN-RING jsou:

- jednoduchost instalace,
- rychlá rekonfigurace (30ms),
- vysoká zatížitelnost (80%),
- jednovláknová WDM technologie [43].

Rozdělení LAN-RING topologie se dále dělí:

- **LAN-RING 200M** – datový tok ≤ 80Mbps, nepočítá se s rozšíření sytému,
- **LAN-RING 2G** – datový tok ≤ 800Mbps.

Switche jsou osazeny dalšími sériovými linkami: RS485, RS422 a RS232. Tyto porty jsou kompatibilní s řadou výrobců, kteří jsou uvedeni v následující tabulce.

Tab. 16. Seznam kompatibilních systémů [43].

Systém	Výrobce	Popis	Sběrnice
ABSOLUTE	Sicurit	Perimetrický zabezpečovací systém	RS485
ACCO-KP-PS	Satel	Systém kontroly vstupu	RS485
APOLLO	Apollo	Integrovaný bezpečnostní systém	RS422
ASSET	Trade Fides	Integrovaný zabezpečovací systém	RS485
ATS	Aritech	Integrovaný zabezpečovací systém	RS485
CORAL	CIAS	Perimetrický zabezpečovací systém	RS485
DIVA	Ateis	Evakuační rozhlasový systém	AUDIO
DOMINUS	Spelza	Integrovaný zabezpečovací systém	RS485
ERMO 482X	CIAS	Perimetrický zabezpečovací systém	RS485
GALAXY	Honeywell	Integrovaný zabezpečovací systém	RS485
GREEN CENT.	Gre. Center	Parkovací systém	RS422
HUB PRO	Honeywell	Systém kontroly vstupu	RS485
MANTA	CIAS	Perimetrický zabezpečovací systém	RS485
PERIDECT	Sieza	Perimetrický zabezpečovací systém	RS232
PYTHAGORAS	CIAS	Perimetrický zabezpečovací systém	RS485
ROGER	ROGER	Systém kontroly vstupu	RS485
STATION ONE	Diamonds Tech.	Perimetrický zabezpečovací systém	RS485
Varya Perimet.	Ronyo	Perimetrický zabezpečovací systém	TCP/IP

Switche od firmy METEL mají integrované přepěťové ochrany, které šetří náklady na dodatečně způsobené škody. Pravidlem pro správný návrh přepěťových ochran se doporučuje:

- odpor uzemnění do 10Ω,
- co nejmenší délka zemního svodu,
- chráněné vodiče se nesmí křížit se nechráněnými,
- nepoužívat k uzemnění hromosvod.

Switche využívají **PoE** (Power over Ethernet), které redukují množství použitých zdrojů. Integrované přepěťové ochrany chrání nejen switche, ale taky další připojené zařízení jako například kamery a servery [43].

Integrace se softwary C4 a SBI

Komunikace se **software C4** je v SNMPv3, které vyhovuje požadavkům normy ČSN EN 50136 jak z hlediska šifrování dat, tak i ochranu proti změně dat (hash). C4 driver podporuje 2 digitální vstupy NC/NO, podporuje vyvážení smyček se stavy: klid, alarm, sabotáž. Driver podporuje 1 relé výstup na zařízení (switch), které může sloužit k ovládání osvětlení, elektronických zámků a zapínaní presetu. Driver podporuje monitorování napájecího napětí, pracovní teploty zařízení a spojení/rozpojení optického kruhu.

Komunikace se **software SBI** je v SNMPv3vyhovuje stejným normativním požadavkům jako SW C4. Driver podporuje 2 digitální vstupy na zařízení (switch), které podporují vyvážení smyček se stavy: klid, alarm, sabotáž, antimasking a porucha. Driver podporuje detekci spojení/rozpojení všech Fast Ethernet FE/ Giga Ethernet GE portů, dále všech optických portů. Podporuje překročení povoleného datového toku ve směru z/do portu [43].

Aplikace SIMULand a VComNET

Aplikace **SIMULand** = management software pro instalaci a provoz IP systému. Využívá grafickou nadstavbu pro ovládání systému., testování správnosti zapojení při instalaci. Monitoruje stav sítě v různých provozech. Využívá protokol SNMPv3, která vyhovuje ČSN EN 50136 (min. 128bit šifrování a min. 128 bit hash). Vše co je nastavitelné ze SIMULandu je nastavitelné přes SNMPv3.

SNMP správce představuje integrační software **a SNMP agent** představuje zařízení. **SNMP** protokol pro komunikaci správce se vzdálenými zařízením umožňuje:

- čtení hodnot ze vzdáleného zařízení,
- zápis hodnost do vzdáleného zařízení,
- odesílaní upozornění (trapy) o stavu zařízení (napětí, teplota).

SNMP – přístup k položkám:

- každá hodnota SNMP je identifikována pomocí OID (Object ID) s vlastnostni:
  - čtení, zápis,
  - číslo, text,
- seznam OID je uložen v MIB (Management Information Base) databázi,
- na žádost správce agent vrací hodnotu nebo nastavuje požadovanou OID položku.

SNMP – typy příkazů:

- příkazy odesílané správcem,
  - **GetRequest** – nejpoužívanější příkaz, vrací požadovanou hodnotu na vzdáleném zařízení,
  - **GetBulk** – příkaz umožňující seskupení několika dotazů, používá se hlavně pro vyčítání obsáhlých tabulek,
  - **SetRequest** – slouží pro nastavení hodnot na vzdáleném zařízení.
- oznámení odesílané agentem,
  - **Trap** – odesílá správci oznámení o překročení nějaké hodnoty [43].

Verze SNMPv3 rozlišuje od předchozích verzí uživatelská práva pro různé uživatele. Je vyžadována časová synchronizace správce s agentem, aby bylo zabráněno podstrčení starých paketů útočníkem. Spojení šifrování s ověřováním integrity zprávy zajišťuje SNMP vysokou ochranu před útoky. **Šifrování SNMPv3** používá asymetrickou šifru (předání klíče pomocí bezpečného spojení) AES, kterou NSA uznala ke kódování nejtajnějších dokumentů. AES využívá délku klíče 128, 192, 256 bitů. Šifra je velmi rychlá a zatím není známo úspěšné prolomení. **Ověřování integrity dat** probíhá dle následujících kroků:

- odesilatel zprávy spočítá z odesílaných dat tzv. hash,
- příjemce zprávy spočítá hash z přijatých dat,
- příjemce porovná otisk hashe odesílatele se svým.

Využívá hashovaní algoritmus SHA1, kde je délka hashe 160 bitů, jeden z nejpoužívanějších algoritmů [43].

Aplikace **VComNet** je určena pro komunikaci aplikací běžících na operačním systému Windows se zařízeními, které jsou připojeny pomocí RS485/RS422/RS232 do systému LAN-RING. Komunikace se zařízeními probíhá pomocí virtuálních sériových portů. Možnost přijímat a odesílat data identifikovatelná pomocí IP adresy. VcomNet pracuje ve dvou režimech USER/ADMINISTRATOR.

Režim **ADMINISTRATOR** vyžaduje administrativní práva, využívá plný přístup do konfigurace, monitorování a k ladění.

Režim **USER** nevyžaduje administrativní práva, má zakázaný přístup do konfigurace a do ladění. Plný přístup má povolen k monitorování [43].

Dílčí závěr

Výstup čtvrté části tvoří návrh integrovaného poplachového systému, který využívá jako integrační zařízení průmyslové switche od výrobce METEL s.r.o. Tento typ zařízení umožňuje projektovat optimalizované IP sítě a integrovat různé bezpečností technologie při použití jednoho optického vlákna. Při instalaci docílíme minimalizace použité kabeláže. Hlavním bezpečnostním prvkem integrovaného systému, je zapojení switche do kruhové topologie s vlastností rekonfigurací datového toku do 30 ms. Možnosti použití průmyslových switchů najdeme i v extrémních podmínkách vnějšího prostředí, jsou použité verze s hliníkovým krytem zajišťující pasivní chlazení a krytí IP65.

Předběžná kalkulace integrovaného poplachového systémů se odhaduje na 310 000,- Kč.

5 KONVERGENCE POPLACHOVÝCH A INFORMAČNÍCH TECHNOLOGII

Konvergence poplachových systémů s ostatními nepoplachovými systémy, je v důsledku rychlého technologického rozvoje na vysoké úrovni. Využívání společných komunikačních protokolů napomáhá k vzájemnému propojení funkcí jednotlivých aplikací. Rychlý technologický pokrok v elektrotechnice přinesl do integrace poplachových a nepoplachových systémů nové možnosti komunikace koncových zařízení. **Otevřené standardy umožňují konvergenci.** To znamená, že uživatel si může vybrat aplikace, které budou důležité pro jeho používaní a nebudou ho ovlivňovat další zbytečné aplikace.

Poplachové systémy jsou uváděny jako samostatná kapitola, která by měla být zachována i do budoucího vývoje. Poplachové aplikace jsou důležitým prvkem pro ochranu života, zdraví, bezpečnosti osob a zvířat, majetku a životního prostředí. Tyto priority jsou mnohem důležitější než nepoplachové aplikace, které jen zvyšují komfort prostředí a efektivně ovlivňují pracovní režim ve výrobě. Budoucí společnost situaci vidí tak, že by nejraději využívali jeden integrovaný systém, který budou ovládat pomocí jednoho rozhraní. Integrovaný systém, který bude spojovat funkce poplachových a nepoplachových aplikací, může v sobě nést nejistotu možného negativního dopadu na poplachové aplikace.

Moderní poplachové a informační technologie využívají protokoly IP (Internet Protocol), které jsou přizpůsobeny přímému zapojení do paketově orientovaných sítí. Nejběžnějším standardem Ethernetu je pracovní skupina IEEE 802.3, tím pádem je systém připravený ke kooperaci s ICT (Information and Communication Technologies) na vyšších vrstvách (aplikační) modelu OSI.

Tab. 17. Model ISO/OSI.

Vrstvy MODEL ISO/OSI	Příklady protokolů
7. Aplikační vrstva	FTP, DNS, DHCP, POP3, SMTP, SSH, Telnet, TFTP
6. Prezentační vrstva	Šifrování, konvertování, komprimace (SMB)
5. Relační vrstva	Povolení přístupu (NetBIOS, Apple Talk, RPC, SSL)
4. Transportní vrstva	TCP,UDP, AEP, SCTP, RTP, AMTP, ATP, CUDP, NBP
3. Síťová vrstva	IPx, ICMP, NWLink, IPsec, ARP, RARP, X.25 PLP, SCCP
2. Linková vrstva	Ethernet, SDLC, HDLC, LAPB, ODI, NDIS, SANAII
1. Fyzická vrstva	1xxBASE-xx, DSL, RS-xxx, USB, IEEE 802., Bluetooth

V důsledku používaného standardu IEEE 802.3. informačních technologii, mohou být funkce poplachových systémů využívány i na jiné aplikace, než je jejich původní záměr použití. Můžeme to chápat tak, že pohybové detektory nebudou sloužit jen k detekci narušení chráněného prostoru, ale také například k počítání průchodu osob, ovládání osvětlení a dalších zařízení, které nespadají pod poplachové aplikace.

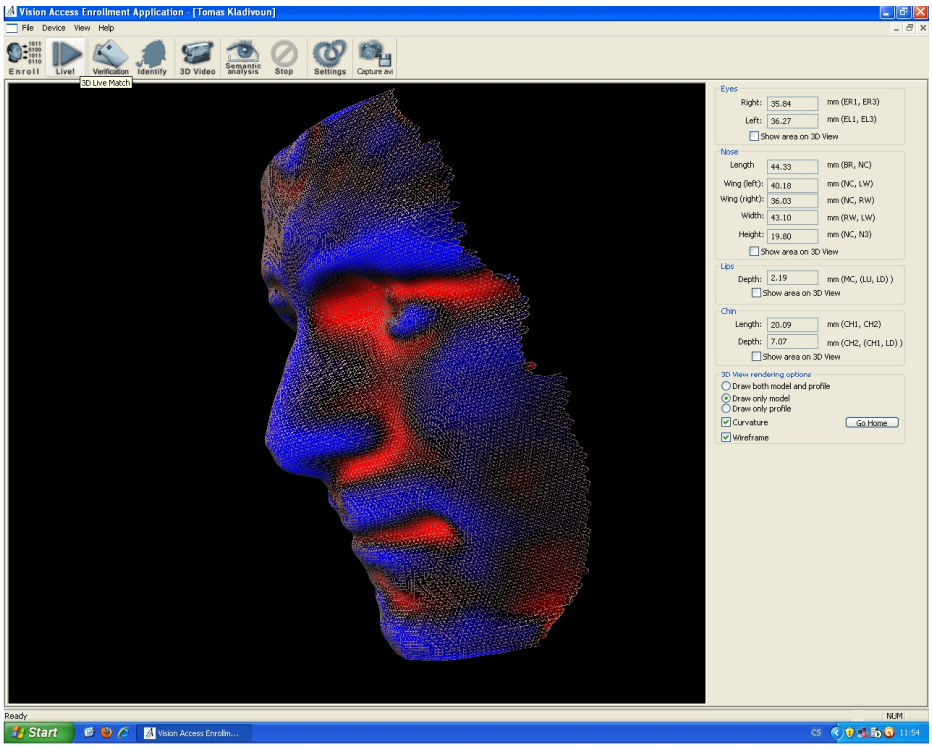
5.1 Vývojové prvky a software

Výzkum a jednotlivá měření fyzikálních vlastností případného pachatele, přispěli k vývoji moderních prvků poplachových systémů s využíváním principů intonační technologie. Vývojové firmy poplachových systému v dnešní době vsází převážně na **vývoj komplexních kamerových systémů.**

5.1.1 Prvky

Využití prvků informační technologie v kamerových systémech, přispělo k moderní analýze snímaného obrazu. Z bezpečnostního hlediska, vývoj kamerové systémy posunul na přední místo použité techniky, při pátrání po nebezpečných osobách. Díky záznamům z bezpečnostních kamer, které jsou umístěny u dálnice a dalších frekventovaných částí vozovky můžeme zaznamenat RZ vozidla, popřípadě portrét řidiče. Kamerová detekce snímaného obrazu je založena na rozpoznání některých biometrických prvků. Moderní technologie dospěly k úspěšnému 3D skenování obličeje. Implementace této metody do kamerového systému, se využívá pro identifikaci podezřelé osoby. Tyto vyspělé kamerové systémy jsou určeny pro objekty s vysokou bezpečnostní hodnotou, jako jsou banky, letiště a armádní objekty. Další možností nasazení kamerových systému, kde využijí nové moderní trendy, jsou obchodní střediska a výrobní podniky. U rozsáhlých obchodních domů, monitorují délku fronty u pokladny, kde systémy sami zpracovávají otevření další pokladny. Použití kamerových aplikací ve výrobním systému podniku, zefektivní případné postupy kontroly výrobky, které mohou být v důsledku lidského faktoru přehlédnuté. Technické zabezpečení velkých měst je založeno na monitorování zájmových míst, kde se vyskytuje velký počet osob nebo místa s možností vzniku konfliktní situace. Kamerové systémy díky vývoji informačních technologii mohou do své databáze zapsat osoby, vozidla, výrobky s jedinečným identifikátorem. Při pohybu osoby po městě jej mohou kamery automaticky

sledovat a předpovídat jeho možnou trasu, výsledkem je účinné pátrání po podezřelých osobách [44].



Obr. 50. 3D snímek obličeje.

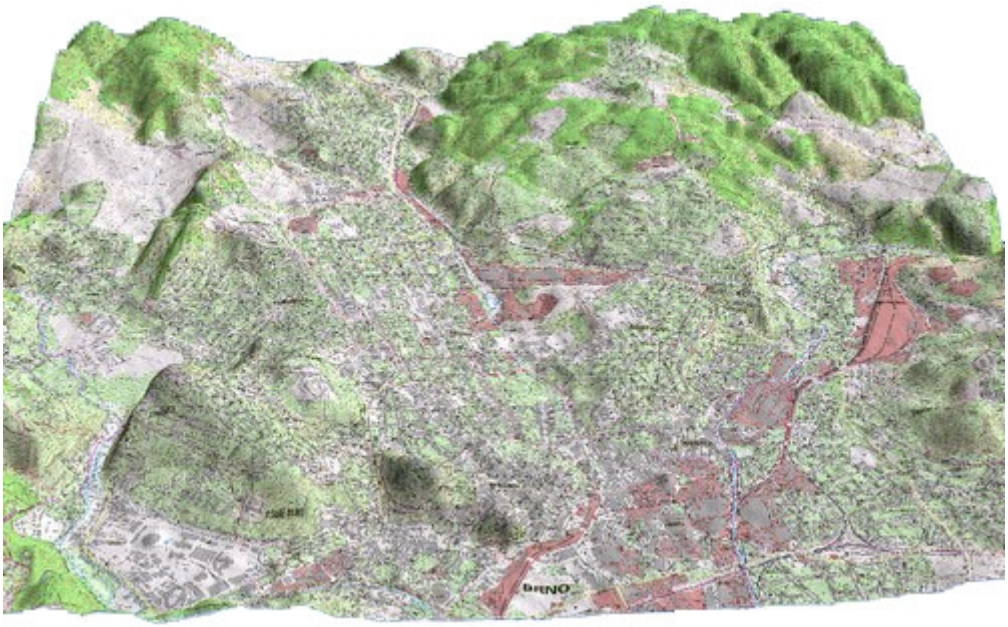
Firmy, které se snaží v kamerových systémech udělat další technologický krok dopředu, vychází z možností jak uspokojit potencionálního zákazníka, ale taky zvyšovat bezpečnostní koeficient celého kamerového systému. Nejvýznamnější firmy ve vývoji kamerových systému jsou: Axis, Siemens, Samsung, Panasonic, Bosch, Sony, a další.

Systémy kontroly přístupu prošly řadou změn díky vývojovým prvkům informační technologie. Převážně identifikace jednotlivých osob je na vyšší úrovni, než tomu bylo dříve. Přístupové karty sice nejsou úplnou minulostí, ale jejich možné zneužití je čím dál tím vice pravděpodobné. Identifikace u moderních přístupových systémů vychází z jedinečných biometrických vlastností člověka. Jednotlivé **biometrické identifikátory**, dokážou přístupové systémy zpracovat díky moderní informační technologii a nahrát do své databáze. Vytěžované biometrické znaky jednotlivých osob jsou převážně z oblasti obličeje, kde se zpracovávají 3D snímky, dále detailní identifikace oční struktury nese v sobě jedinečné identifikační znaky. Další vyspělou identifikační metodou u přístupových systémů je **bipedální lokomoce**, která vychází z pohybového systému člověka. Na základě počítačové simulace, lze jedinečné pohyby při chůzi identifikovat a tím rozpoznat jednotlivé

osoby. Další vývojový stupeň biometrických vlastností člověka je **identifikace krevního řečiště**. Převážně se vychází z krevního řečitě ruky, která je díky speciálním senzorům naskenována do databáze přístupových systémů. Další identifikační znaky umístěné na ruce jsou otisky prstů, které jsou v dnešní době běžnou záležitostí přístupových systémů. Jednotlivá data z přístupových systémů lze exportovat do systémů vyšší organizační struktury firmy, která následně přijatá data může zpracovávat například na mzdový systém, využívání efektivního pracovního prostoru a strojů.

5.1.2 Software

Vývoj na straně prvku poplachových systému, nám přináší větší komplexnost manipulace se softwary jednotlivých aplikací. Moderní SW jsou vhodné pro ovládání a monitorování integrovaného systému v místě s vysokou zabezpečovací hodnotou. Software je závislý na vzájemném propojení funkcí poplachových aplikací. Každý poplachový systém má výstupní data ve formátu, se kterým lze dále manipulovat pro následné zpracování požadované informace. Využitím moderních prvku informační technologie můžeme požadované informace zobrazit v různých podobách od klasických monitorů po plastické mapy, 3D obrazy a zobrazovací tabla. Formát výstupních dat má vliv na ovládací a monitorovací schopnosti poplachových systémů a možnou reakci na danou situaci.



Obr. 51. 3D mapa [45].

Softwary zpracovávají informace, které následně mohou sloužit k vizualizaci nebo dalšímu zpracování odesílaných dat. Konvergence SW funkcí můžeme sledovat převážně u těchto aplikací:

- okruh PZTS, ACS, EPS, CCTV, Enviro,
- ovládání pomocí mobilního telefonu, správa návštěv, recepce,
- docházkový systém, výdaje stravenek, grafické plánování,
- nastavení pracovních ploch, export do mzdových systémů.

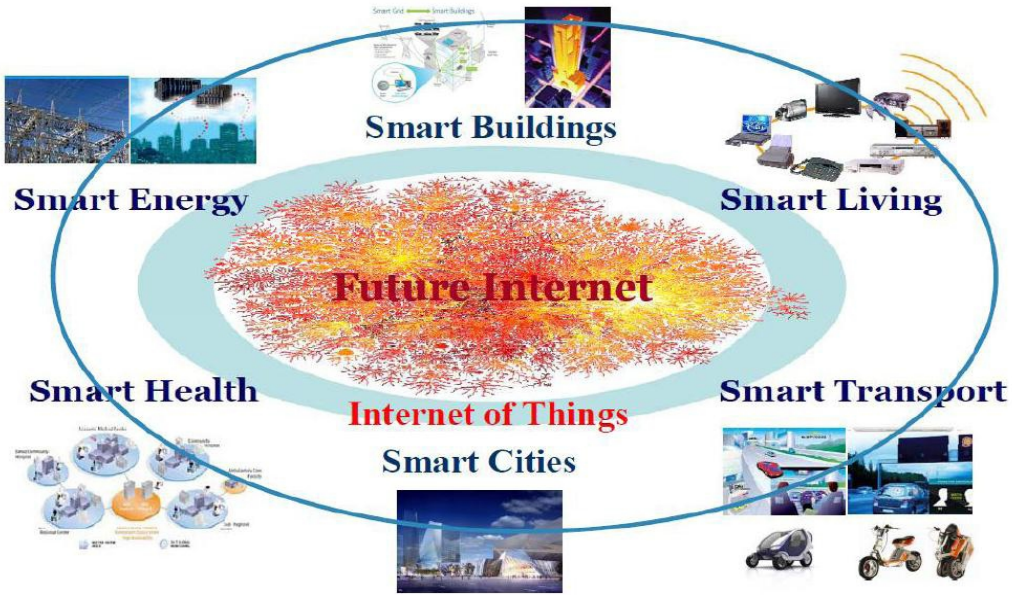
I když propojení nepoplachových aplikací s poplachovými aplikacemi, může vnést do softwarové část systému rozpory v ovládání jednotlivých funkcí systémů. Jen díky otevřeným standardům se docílí konvergence propojených systémů. Konvergence SW části budou mít v budoucnu převážně uplatnění v integraci městských systému, na které jsou kladeny vysoké požadavky z hlediska kvality pořizovaného záznamu a přenosu dat na velkou vzdálenost.

5.2 Strategie směrování vývoje

Vycházíme ze tří základních oblastí směřování vývoje. Strategie oblastí jsou následující:

- identifikace problémových míst - stávající standarty nesplňují požadavky,
- zabránění možným rozporům ve standardizaci,
- vertikální propojení přes různá obchodní řešení a průmyslová odvětví.

Příležitosti zrychlení procesu standardizace a rozšíření příležitosti obchodu díky rozvoji M2M (machine-to-machine). Ustálená standardizace koncových zařízená M2M a jejich globální spolupráce umožňující nadstavby. Vytvoření globálně aplikovatelných standardů, které budou akceptovat regionální požadavky a vertikální potřeby trhu (adaptace). Nové obchodní příležitosti díky zastřešení a komunikaci stávajících technologií [46].



Obr. 52. Nová příležitost k vertikálnímu propojení technologií a jejich aplikací [46].

Komunikace Machine to Machine (M2M)

M2M je podřízeno takzvaným **internetem věcí**, které představuje prostředí inteligentních přístrojů připojených do internetu s možností jejich ovládání a přístupu k datům na dálku. Současný nárůst bezdrátové komunikace a cloud computingu otevírá komunikační prostor pro jeho reálný rozvoj. Integrace „chytrých objektů“, v rámci internetu umožní vzájemnou komunikaci.

Praktické využití je obrovské – od **optimalizace** nákladů a nové úrovně **ovládání** předmětů na dálku, přes průmyslové **měřící** systémy až po vznik speciálních služeb na míru. Již běžnou záležitostí jsou různé lékařské přístroje monitorující stav pacienta a posílající data do centrálního systému, který je případně spojen s tísňovým systémem přivolání pomoci. V podnikové sféře lze integrovat data z inteligentních zařízení přímo do informačních systémů a provádět nad nimi hloubkové analýzy. **Výsledkem** bude inteligence všude kolem nás, kde se stále častěji budeme setkávat s objekty jako inteligentní domy, chytré elektrické zařízení nebo inteligentní automobily [47].

Dílčí závěr

Konvergence poplachových a informačních technologií je na vzájemném vzestupu díky celosvětově rozšířené komunikační sítí internet. Pomocí kterého dokážeme navázat komunikaci mezi vzdálenými objekty. V dnešní době je hlavním nebezpečím zneužití pořízených informací z jednotlivých systémů, které jsou shromažďovány na jednom úložišti dat. U konvergence prvků lze předpokládat spíše vývoj k minimalizaci a mobilitě, použití špičkových zařízení do extrémních podmínek. Díky informační technologii, zpracování informací z vnějšího prostředí probíhá na vysoké úrovni, které vychází z fyzických vlastností střeženého/monitorovaného prostoru. Předpokládané způsoby konvergence na softwarové úrovni se budou odvíjet od ovládání systému uživatelem. Nejvyšší možné provázání systému nám umožní prvky informační technologie. Ve výsledku propojení jednotlivých funkcí aplikací je důležité jaké informace z koncových zařízení budeme přijímat a zpět odesílat (akce/reakce).

ZÁVĚR

Usnesení jednotlivých legislativních požadavků týkající se integrovaných poplachových systémů, představují podrobné informace o průběžných činnostech při zřizování IPS. Legislativa ovlivňuje výrobce, dovozce a prodejce komponentů, které jsou nezbytné pro IPS. Ve výsledku je důležité dbát na splnění požadavků zákazníka a k tomu dodržovat platné technické a legislativní požadavky, které budou zvyšovat svou úroveň, díky vývoji nových poplachových a informačních technologií.

Všechna společná zařízení v integrovaném systému musí splňovat technické požadavky, které jsou stručně obsaženy v příslušné normě ČSN CLC/TS 50398. Tato norma se sice dále odkazuje na jednotlivé normy příslušných poplachových systémů, ale technické požadavky na vzájemné propojení poplachových funkcí norma nepředstavuje skoro vůbec. V důsledku rychlého rozvoje integrovaných systému, norma nemá žádné stanoviska pro systémy využívající prvky informační technologie. Převážně vývoj v oblasti informační technologie je na vzestupu a bude se využívat pro integraci systémů. Jelikož dokážou zpracovat více druhu komunikačních formátu z oboru informační technologie, jsou ideálním řešením do budoucnosti z hlediska konfigurace a konvergence.

Integrace poplachových systému se vyznačuje propojením funkcí, které slouží k ochraně majetku a osob. V závislosti na charakteru propojených poplachových aplikací, může určit sílu provázanosti použitých systémů. Nejvyšší úroveň komunikace koncových zařízení je přizpůsobena použití integračních prvků, využívající informační technologii.

Proč právě prvky informační technologie umožňují komunikaci na tak vysoké úrovni? Jelikož využívají standardy, které se používají v dnešním internetovém světě. Tyto standardy mají požadavky postaveny na vysoké přenosové rychlosti a bezpečném přenosu dat z jednoho zařízení do druhého. Určité bezpečnostní riziko je u datových úložišť, které uchovávají velké množství citlivých údajů týkající se střežených objektů. V případě zneužití citlivých dat, hrozí větší rozsah způsobených škod, než u autonomních systémů.

S konvergencí poplachových a informačních technologii musíme počítat do budoucna. V nastávající době budou integrované systémy procházet vzájemným překrýváním funkcí každého použitého zařízení. Samostatná „inteligentní“ zařízení budou obstarávat více funkcí, než jim bylo přidělováno do této chvíle. Moderní integrované systémy budoucnosti budou vstupovat přímo do podvědomí společnosti lidí, díky jejich širokému spektru

působnosti. Tento posun v této chvíli je prakticky nezadržitelný a je jen na nás, jak připravíme klíčové podmínky dnešní společnosti pro integrovaný systém.

ZÁVĚR V ANGLIČTINĚ

Resolution of legal requirements regarding integrated alarm systems are details about the ongoing activities in the establishment IPS. Legislation affecting the manufacturer, importer and distributor of components that are necessary for IPS. As a result, it is important to ensure compliance with customer requirements and comply with the applicable technical and legislative requirements, which will raise your level, thanks to the development of new alarms and information technology.

All common facilities in an integrated system must satisfy the technical requirements, which are briefly covered in the standard ČSN CLC/TS 50398. This standard, while also refers to various standards appropriate alarm systems, but the technical requirements for the interconnection of alarm functions standard is not much at all. With the rapid development of integrated systems, standards have no opinion for systems using elements of information technology. Mostly developments in information technology is on the rise and it will be used for systems integration. As can handle multiple types of communication formats in the field of information technology are the ideal solution for the future in terms of configuration and convergence.

Integration alarm system is characterized by linking features that serve to protect persons and property. Depending on the nature of the related alarm applications can determine the strength of the interconnection systems. The highest level of communication terminal equipment is adapted to use integration elements, using information technology.

Why elements of information technology enable communication at such a high level? Since the use of standards in use in today's Internet world. These standards are based on the requirements of high transmission speed and secure data transfer from one device to another. A security risk for data warehouses, which store large amounts of sensitive data on the guarded objects. In case of misuse of sensitive data, there is a greater extent of the damage than at autonomous systems.

With the convergence of alarm and information technology we expect in the future. In the coming time, the integrated systems go through overlapping functions of each of the devices. Independent „inteligent“ devices will cater more features than they were allocated to this moment. Modern integrated systems of the future will enter directly into the subconscious of people, thanks to their wide range of application. This shift in this moment

is virtually unstoppable and it is up to us to prepare today's key conditions of the integrated system.

SEZNAM POUŽITÉ LITERATURY

[1] BRADÁČOVÁ, Isabela. SDRUŽENÍ POŽÁRNÍHO A BEZPEČNOSTNÍHO INŽENÝRSTVÍ. *Požární bezpečnost staveb: Nevýrobní objekty*. Frýdek Místek: Tiskárna Kleinwachter, 2007. Spbi spektrum 50. ISBN 978-80-7385-023-4.

[2] Česká republika. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In *Sbírka zákonů*. 2000, 32.

[3]Oblasti zpracování osobních údajů. *Úřad pro ochranu osobních údajů* [online]. [cit. 2013-03-03]. Dostupné z: http://www.uoou.cz/

[4]Česká republika. Zákon č. 133/1985 Sb., o požární ochraně. In *sbírka zákonů*. 1985, 34.

[5]Česká republika. Zákon č. 183/2006 Sb., o územním plánování a stavebním řádu (stavební zákon), ve znění pozdějších předpisů. In *Sbírka zákonů.* 2006, 64.

[6] Česká republika. Vyhláška č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci). In *Sbírka zákonů*. 2001, 95.

[7] Česká republika. Vyhláška č. 23/2008 Sb., o technických podmínkách požární ochrany staveb. In *Sbírka zákonů*. 2008, 10.

[8]*Studijní materiály: Přednášky PIS*. Zlín, 2012. Zápisky. UTB ve Zlíně.

[9]Česká republika. Zákon č. 102/2001 Sb., Zákon o obecné bezpečnosti výrobků a o změně některých zákonů (zákon o obecné bezpečnosti výrobků). In *Sbírka zákonů*. 2001, 41.

[10] BRURANT, Jiří a Lumír BRABEC. *Požární bezpečnost elektrických instalací*. Praha: IN - EL, 2004. Knižnice Elektro, svazek 72. ISBN 80-86230-33-3.

[11]Česká republika. Zákon č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů. In *Sbírka zákonů.* 2007, 6.

[12]Česká republika. Nařízení vlády 17/2003 Sb., kterým se stanoví technické požadavky na elektrická zařízení nízkého napětí. In *Sbírka zákonů*. 2003, 9.

[13]Česká republika. Nařízení vlády 616/2006 Sb. o technických požadavcích na výrobky z hlediska jejich elektromagnetické kompatibility. In *Sbírka zákonů*. 2006, 191.

[14]Česká republika. Nařízení vlády 426/2000 Sb., kterým se stanoví technické požadavky na rádiová a na telekomunikační koncová zařízení. In *Sbírka zákonů*. 2000, 119.

[15]Česká republika. Zákon č. 360/1992 Sb., o výkonu povolání autorizovaných architektů a o výkonu povolání autorizovaných inženýrů a techniků činných ve výstavbě. In *Sbírka zákonů*. 1991, 87.

[16]Česká republika. Zákon č. 455/1991 Sb., o živnostenském podnikání. In *Sbírka zákonů*. 1991,87.

[17]Česká republika. Nařízení vlády č. 278/2008 Sb., o obsahových náplních jednotlivých živností. In *Sbírka zákonů*. 2008, 94.

[18]Česká republika. Vyhláška č. 50/1978 Sb., Českého úřadu bezpečnosti práce a Českého báňského úřadu o odborné způsobilosti v elektrotechnice. In *Sbírka zákonů*. 1978, 11.

[19]Úřad pro technickou normalizaci, metrologii a státní zkušebnictví [online]. [citováno 2013-03-03]. Dostupné z http://www unmz.cz.

[20]VALOUCH, Jan. Projektování bezpečnostních systémů. [skriptum]. Zlín: UTB, 2012. ISBN 978-80-7454-230-5. 152 s.

[21]ČSN CLC/TS 50 131-7. *Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. 44 s.

[22]ČSN EN 50 132-7. *Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích – Část 7: Pokyny pro aplikace.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010. Třídící znak 33 4592.

[23]ČSN EN 50 133-7. *Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích – Část 7: Pokyny pro aplikace.* Praha: Český normalizační institut, 2001. Třídící znak 33 4593.

[24]ČSN EN50 134-1. *Poplachové systémy – Systémy přivolání pomoci – Část 1: systémové požadavky.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2003. Třídící znak 33 4590.

[25]ČSN EN 50 136-1. *Poplachové systémy – Poplachové přenosové systémy a zařízení – - Část 1: Obecné požadavky na poplachové přenosové systémy.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012. Třídící znak 33 4596.

[26]ČSN CLC/TS 50398. *Poplachové systémy – Kombinované a integrované systémy – Všeobecné požadavky.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. Třídící znak 33 4597.

[27]ČSN EN 50 130-5. *Poplachové systémy – Část 1: Metody zkoušek vlivu prostředí.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2001. Třídící znak 33 4590.

[28]ČSN EN 50 130-4. *Poplachové systémy – Část 4: Elektromagnetická kompatibilita – Norma skupiny výrobků: Požadavky na odolnost komponentů požárních systémů, poplachových zabezpečovacích a tísňových systémů a systémů CCTV, kontroly vstupu a přivolání pomoci.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012. Třídící znak 33 4590.

[29]ADI GLOBAL DISTRIBUTION BRNO. *Zásady integrace bezpečnostních a řídicích systémů*. Praha, 2010.

[30]ASOCIACE GRÉMIUM ALARM. *Komise Integrovaných systémů*. 2010. Dostupné z: http://www.gremiumalarm.cz/.

[31]INELS. *Systém inteligentní elektroinstalace* [online]. 2013 [cit. 2013-04-26]. Dostupné z: http://www.inels.cz/

[32] DUŠEK, Bedřich. JOHNSON CONTROL. *Teorie a praxe inteligentních budov*. 2012.

[33]PARADOX. *GPRS / GSM / IP / Voice – IPR512*. 2013. Dostupné z: http://www.paradox.com/Products/.

[34]METASYS BUILDING MANAGEMENT SYSTEMS. *Johnson Control* [online]. 2013 [cit. 2013-05-02]. Dostupné z: http://www.johnsoncontrols.co.uk/.

[35] SLACH, Martin. SIEMENS. *Integrace bezpečnostních systémů*. 2012.

[36] Siemens. *Produkty pro požární a bezpečnostní systémy* [online]. 2013 [cit. 2013-05-02]. Dostupné z: http://www.siemens.com/.

[37]HW GROUP. *HWg-STE: Ethernet teploměr* [online]. 2012 [cit. 2013-05-02]. Dostupné z: http://www.hw-group.com/products/HWg-STE/.

[38]VARIANT. *Obor ISB: VAR-NET INTEGRAL* [online]. 2010 [cit. 2013-05-02]. Dostupné z: http://www.variant.cz/dokumenty/obor-isb/.

[39]HW-GROUP. *Síťové komunikační protokoly* [online]. 2010 [cit. 2013-05-02]. Dostupné z: http://www.hw-group.com/products/poseidon/pos_protocols_cz.html.

[40]AUTOMATIZACE HW. *Úvod do BACnetu* [online]. 2010 [cit. 2013-05-02]. Dostupné z: http://automatizace.hw.cz/uvod-do-bacnetu-building-automation-and-controls-network.

[41]WIKIPEDIE. *M-Bus* [online]. 2012 [cit. 2013-05-02]. Dostupné z: http://cs.wikipedia.org/wiki/M-Bus.

[42]HERMANN, Merz, THOMAS, Hansemann a CHRISTOF, Hübner. Automatizované systémy budov: Sdělovací systémy KNX/EIB, LON a BACnet. Praha: Grada, 2009. Edice Stavitel. 264s. ISBM 978-80-247-2367-9.

[43] *Managed switch.* Česká skalice: Metel s.r.o, 2013.36 s.

[44] IP kamera AXIS P5414-E. ORSEC. *Bezpečnostní portál* [online]. 2013 [cit. 2013-05-25]. Dostupné z: http://www.orsec.cz/cs/informacni-servis/ip-kamera-axis-p5414-e_138-1702/.

[45]*OziExplorer3D* [online]. 2012 [cit. 2013-05-25]. Dostupné z: http://www.technika.ilcik.cz/system-gps/programy/oziexplorer3d/index.html.

[46]VOJTĚCH, Lukáš. CZECH TECHNICAL UNIVERSITY IN PRAGUE. *Internet věcí: deštník nad inteligentními subsystémy*. 2012.

[47]PASTUCHOVÁ, Markéta. M2M komunikace: Přínosy a rizika internetu věcí. *ICT manager* [online]. 2012 [cit. 2013-05-25]. Dostupné z: http://www.ictmanazer.cz/2012/03/m2m-komunikace-prinosy-a-rizika-internetu-veci/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

PZTS	Poplachový zabezpečovací a tísňový systém.
ACS	Systém kontroly vstupu.
CCTV	Uzavřený televizní okruh pro bezpečnostní aplikace.
SAS	Systém přivolání pomoci.
EPS	Elektrická požární signalizace.
NV	Nařízení vlády.
Sb.	Sbírka.
ČSN	Česká technická norma.
EN	Evropská norma.
CLC/TS	Cenelec / Technická specifikace.
ES	Evropská směrnice.
CE	Prohlášení o shodě.
GSM	Globální systém pro mobilní komunikaci.
OSVČ	Osoba samostatně výdělečně činná.
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.
EU	Evropská unie.
TNI	Technická normalizační informace.
IPS	Integrovaný poplachový systém.
I&HAS	Intruder and Hold-up Alarm System.
IP	Internet Protocol.
RZ	Registrační značka.
DPPC	Dohledové a poplachové přijímací centrum.
ATS	Poplachový přenosový systém.
CCF	Centrální ovládací zařízení.

EMC	Elektromagnetická kompatibilita.
IT	Informační technologie,
A/V	Audio/video.
SW	Software.
HW	Hardware.
BMS	Building Management System.
LAN	Local Area Network.
WAN	Wide Area Network.
GPRS	General Packet Radio Service.
RFID	Radio frequency identification.
FTP	File Transfer Protocol.
DVR	Digital video recorder.
HTTP	Hypertext Transfer Protocol Secure.
ARP	Address Resolution Protocol.
UDP	User Datagram Protocol.
TCP	Transmission Control Protocol.
DHCP	Dynamic Host Configuration Protocol.
SNMP	Simple Network Management Protocol.
SMTP	Simple Mail Transfer Protocol.
SNTP	Simple Network Time Protocol.
IGMP	Internet Group Management Protocol.
UPNP	Universal Plug and Play.
TÜV	Technischer Überwachungs – Verein.
WDM	Wavelength – division multiplexing.
FE	Fast Ethernet.

PoE	Power over Ethernet.
MM	Multimode.
SM	Singlemde.
M2M	Machine to Machine.
Gbps	Gigabit per second.
Mbps	Megabit per second.
IEEE	Institute of Electrical and Electronics Engineers.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: CERTIFIKÁT O ABSOLVOVÁNÍ ŠKOLENÍ .

www.metel.eu

METEL s.r.o.

vydává

CERTIFIKÁT
O ABSOLVOVÁNÍ ŠKOLENÍ

Projektování, instalace a servis
IP systémů LAN-RING

Úroveň: (X) projektování o délce 5 hodin

( ) instalace a servis o délce _ hodin

Tímto certifikátem stvrzujeme, že

pan(í): Tomáš MACHAČ

z firmy: UTB Zlín

absolvoval(a) výše uvedené školení, které bylo zaměřeno zejména na získání znalostí nutných k projektování, instalaci a servisu IP produktů fy METEL s.r.o.

Za METEL s.r.o.: .....
Tomáš Metelka
technický ředitel

V České Skalici, dne: 4.4.2013

METEL s.r.o., Žižkův Kopec 617, 552 03 Česká Skalice; www.metel.eu