

# **Možnosti zabezpečení budovy U5 na UTB ve Zlíně**

Vlastimil Krejčí



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2015/2016

## **ZADÁNÍ BAKALÁŘSKÉ PRÁCE**

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Vlastimil Krejčí**  
Osobní číslo: **A13266**  
Studijní program: **B3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**  
Forma studia: **kombinovaná**

Téma práce: **Možnosti zabezpečení budovy U5 na UTB ve Zlíně**  
Téma anglicky: **Security Possibilities for the U5 Building at TBU in Zlín**

Zásady pro vypracování:

1. Zpracujte přehled a analýzu technologií pro zabezpečení školních budov.
2. Představte legislativní předpisy pro přístupové systémy.
3. Analyzujte současný stav zabezpečení budovy U5, FAI UTB, ve vztahu k průchodu nežádoucích osob.
4. Navrhněte doplnění současného stavu zabezpečení.
5. Provedte ekonomickou rozvahu navrženého řešení.

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 3. Blatná: Cricetus, 2006, 313 s. ISBN 8090293824.
2. UHLÁŘ, Jan. Technická ochrana objektů. Vyd. 1. Praha: Vydavatelství PA ČR, 2005, 229 s. ISBN 8072511890.
3. VALOUCH, Jan. Projektování bezpečnostních systémů. 1. Zlín: Univerzita Tomáše Bati, 2002. ISBN 978-80-7454-230-5.
4. LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Vyd. 1. Zlín: Univerzita Tomáše Bati, Fakulta technologická, 2003, 64 s. ISBN 8073181193.
5. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 9788087500057.

Vedoucí bakalářské práce:

**Ing. Libor Pekař, Ph.D.**

Ústav automatizace a řídicí techniky

Datum zadání bakalářské práce:

**26. února 2016**

Termín odevzdání bakalářské práce:

**30. května 2016**

Ve Zlíně dne 16. února 2016

doc. Mgr. Milan Adámek, Ph.D.  
*děkan*



Ing. Jan Valouch, Ph.D.  
*ředitel ústavu*

### **Prohlašuji, že**

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

### **Prohlašuji,**

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

Ve Zlíně, dne

27.5.2016

  
.....  
podpis diplomanta

## **ABSTRAKT**

Hlavním tématem bakalářské práce je popis současného stavu zabezpečení budovy U5 (Fakulta aplikované informatiky UTB ve Zlíně) a návrh technického řešení ve vztahu k průchodu a pohybu osob v budově, využití identifikačních prvků a databází uživatelů pro další systémy. Teoretická část zpracovává přehled a analýzu nejdůležitějších technologií pro zabezpečení školních budov. Seznamuje s hlavními legislativními předpisy a technickými požadavky na vybrané technologie. V praktické části popisuje návrh možnosti lepšího zabezpečení budovy U5 na UTB ve Zlíně. Důraz je kladen na kontrolu příchozích a odchozích osob. Zohledňuje doplnění technologií pro možnost bezbariérového užívání budovy. Součástí práce je nabídka realizace navrženého systému i s ekonomickým zhodnocením.

Klíčová slova: Systémy kontroly vstupu, přístupové systémy, ACCESS, Kombinované a integrované systémy, Identity management.

## **ABSTRACT**

The main topic of this bachelor thesis is a description of a current condition of security of building U5 and a concept of technical solution in relation to passage and movement of people in the building, use of identification elements and database for another systems. In the theoretical part summary and analysis of the most important technologies for securing of school buildings are concerned. Further there are main law regulations and technical requirements of certain technologies mentioned. In the practical part a draft of improved security of the building U5 at TBU in Zlín is described. In the thesis the check of incoming and outgoing persons is emphasized. It also consists of an additional technology for the possibility of barrier-free use of the building. In another part of the thesis an offer of the implementation of designed system including economic assessment is comprised.

Keywords: Access control systems, access systems, Access, Combined and integrated systems, Identity management.

Na tomto místě chci poděkovat panu Ing. Liboru Pekařovi za ochotu, cenné rady a jeho čas věnovaný mé práci.

Také chci poděkovat firmám Cominfo a.s. Zlín a Trade FIDES a.s. Brno za cenné informace a podklady.

V neposlední řadě děkuji mé rodině za velkou trpělivost a podporu během celého studia.

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

# OBSAH

<b>ÚVOD.....</b>	<b>10</b>
<b>I TEORETICKÁ ČÁST.....</b>	<b>11</b>
<b>1 ZABEZPEČENÍ ŠKOLNÍCH BUDOV .....</b>	<b>12</b>
1.1 ELEKTRONICKÉ ZABEZPEČOVACÍ SYSTÉMY – SKV, PZTS, CCTV .....	13
1.2 ELEKTRONICKÉ SYSTÉMY KONTROLY VSTUPU .....	13
1.2.1 Terminologie SKV .....	14
1.2.2 Topologie .....	15
1.2.3 Identifikace.....	17
1.2.4 Role .....	18
1.2.5 Identifikační prvky .....	19
1.2.6 Snímací zařízení .....	23
1.2.7 Ovládaná zařízení.....	23
1.3 POPLACHOVÉ ZABEZPEČOVACÍ A TÍŠŇOVÉ SYSTÉMY PZTS.....	24
1.3.1 Terminologie .....	24
1.3.2 Topologie .....	25
1.3.3 Detektory.....	27
1.4 INTEGRACE.....	27
1.5 IDENTITY MANAGMENT .....	28
1.5.1 Definice .....	28
1.5.2 Architektura.....	29
1.5.3 SSL (Secure sockets Layer) a TLS (Transport Layer Security) .....	30
<b>2 LEGISLATIVA .....</b>	<b>32</b>
2.1 ACS - SYSTÉMY KONTROLY VSTUPU .....	33
2.1.1 Třídy identifikace .....	34
2.1.2 Třídy přístupu.....	35
2.1.3 Návrh systémů kontroly vstupu .....	35
2.2 POPLACHOVÉ SYSTÉMY – KOMBINOVANÉ A INTEGROVANÉ SYSTÉMY.....	38
2.2.1 Typy konfigurací .....	38
2.2.2 Systémové požadavky .....	39
<b>II PRAKTICKÁ ČÁST .....</b>	<b>40</b>
<b>3 ZABEZPEČENÍ BUDOVY U5 .....</b>	<b>41</b>
3.1 ÚVOD .....	41
3.1.1 Identifikační údaje stavby .....	41
3.1.2 Podklady.....	41
3.1.3 Situace .....	41
3.2 ZÁKLADNÍ TECHNICKÉ ÚDAJE .....	42
3.2.1 Rozvodné soustavy.....	42
3.2.2 Ochrana před úrazem elektrickým proudem .....	43
3.2.3 Prostředí dle ČSN EN 50131-1 .....	43
3.3 ZHODNOCENÍ RIZIK .....	43
3.4 STÁVAJÍCÍ ELEKTRONICKÉ ZABEZPEČOVACÍ SYSTÉMY .....	44
3.4.1 PZTS .....	44
3.4.2 SKV.....	45

3.4.3	CCTV .....	46
3.4.4	DZ .....	48
3.4.5	EPS .....	48
3.4.6	MZP.....	50
3.4.7	Fyzická ostraha, režimová opatření.....	50
3.5	ZHODNOCENÍ.....	50
<b>4</b>	<b>NÁVRH DOPLNĚNÍ ZABEZPEČENÍ.....</b>	<b>52</b>
4.1	ÚVOD .....	52
4.2	DOPLNĚNÍ STÁVAJÍCÍ TECHNOLOGIE.....	52
4.2.1	Doplnění SKV .....	52
4.2.1.1	Doplnění snímacích zařízení k samostatným vstupům .....	53
4.2.1.2	Doplnění turniketů .....	53
4.2.1.3	Ovládání.....	54
4.2.1.4	CCTV People Counter .....	54
4.2.1.5	Návrhy prvků .....	55
4.2.2	Doplnění PZTS.....	55
4.2.2.1	Návrhy prvků .....	57
4.2.3	Doplnění CCTV .....	57
4.2.3.1	Návrhy prvků .....	59
4.2.4	Provoz kamerového systému.....	59
4.2.5	Úprava MZP .....	59
4.2.6	Integrovaný, monitorovací a řídicí systém, grafická nástavba PZTS, SKV, EPS .....	60
4.2.6.1	Návrh prvků .....	62
4.3	NÁVRH - NOVÁ TECHNOLOGIE .....	63
4.3.1	Popis technologie .....	63
4.3.2	Technické řešení PZTS, SKV .....	65
4.3.2.1	Návrh prvků .....	65
4.3.3	Integrovaný systém .....	66
4.3.4	Rozvody, Kabeláž .....	66
4.3.5	Napájení .....	66
4.4	REALIZACE, UVEDENÍ DO PROVOZU, PROVOZ, ÚDRŽBA .....	67
4.4.1	Návrh provozních předpisů .....	67
4.5	NÁVRH SMLOUVY.....	68
4.5.1	Smlouva o dílo .....	68
4.5.2	Servisní smlouva .....	70
<b>5</b>	<b>ROZVAHA.....</b>	<b>73</b>
5.1	REKAPITULACE .....	73
5.1.1	Rekapitulace dle technologií .....	73
5.2	MOŽNÉ ZPŮSOBY FINANCOVÁNÍ.....	75
5.2.1	Dotační programy MŠMT ČR .....	75
5.2.2	Dotační programy MMR ČR .....	76
5.2.3	Dotační programy MF ČR .....	76
5.2.4	Financování jako službu.....	76
5.3	DOPORUČENÝ POSTUP VÝSTAVBY .....	76
<b>6</b>	<b>ZÁVĚR.....</b>	<b>77</b>



<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>78</b>
<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>81</b>
<b>SEZNAM OBRÁZKŮ .....</b>	<b>82</b>
<b>SEZNAM TABULEK.....</b>	<b>83</b>
<b>SEZNAM PŘÍLOH.....</b>	<b>84</b>

## ÚVOD

Sídlem Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně je budova U5. Budova U5 se nachází v městské části Jižní svahy, na ulici Nad Stráněmi 4511. V budově nyní sídlí Fakulta aplikované informatiky, Fakulta technologická, Fakulta managementu a ekonomiky a menza. Původně byla budova, ve které nyní sídlí FAI UTB, používána jako základní škola. Poslední rekonstrukce budovy proběhla v roce 2004 a ze stejného roku je i stávající zabezpečení budovy. S ohledem na současný vývoj moderních technologií, ale i bezpečnostní situaci, by bylo vhodné zabezpečení budovy modernizovat a zajistit tak větší bezpečnost studentů, pedagogů a ostatních zaměstnanců školy.

Ve své práci „Možnosti zabezpečení budovy U5 na UTB ve Zlíně“ zhodnotím vybrané současné prostředky pro zabezpečení budov. Předložím důležité části legislativních předpisů dotýkajících se těchto oblastí. V praktické části zhodnotím stávající stav zabezpečení MZP, systémy PZTS, ACS, CCTV. Provedu návrh technického řešení pro zlepšení zabezpečení budovy proti neoprávněnému vstupu nežádoucích osob. Součástí práce je návrh skladby systému, který zahrnuje i návrh rozmístění prvků a finanční rozvahu.

## **I. TEORETICKÁ ČÁST**

## 1 ZABEZPEČENÍ ŠKOLNÍCH BUDOV

Za počátek školství v českých zemích a Evropě se dá bezesporu pokládat období Jana Amose Komenského, který svojí činností a úsilím přinášel nejen nové prvky výuky, ale také přispěl ke vzniku prvních „provozních řádů“ ve školách. Ten jako první „Všeobecný školní řád“ vydala v r. 1774 za své vlády až Marie Terezie. Zavedla povinnou školní docházku, což bylo považováno za největší reformu ve školství [1]. Spolu s postupným vývojem školství docházelo k potřebě nějakým způsobem ochránit majetek škol. Nejjednodušší způsob zabezpečení bylo uzamčení školní budovy, postupně pak umístění důležitých předmětů do samostatně uzamykatelné místnosti s jednoduchým mechanickým zamykacím systémem. V průběhu století se vyvíjela důmyslnost a technické provedení mechanických zamykacích systémů spolu s evidencí jejich klíčů. S příchodem moderních technologií se mění také vybavení školních tříd a laboratorních učeben, které jsou v dnešní době nezbytné pro výuku. Bohužel se stávají často nepřekonatelným lákadlem pro řadu nenechavců. V souvislosti s novými technologiemi se setkáváme s elektronicky řízenými mechanickými zámky a elektronickou kontrolou vstupu. Moderní technologie, včetně bezpečnostních, se stávají běžnou součástí nejen rodinných domů již při jejich výstavbě.

Potřeba zlepšovat zabezpečení budov, a to nejen ve školství, je patrna ze statistik PČR. V roce 2015 počet krádeží vloupáním v ČR klesl z 49304 na 34 476 tj. o 14828 vloupání. V tomto směru lze říci, že elektronické zabezpečovací systémy přispívají k poklesu počtu těchto skutků [2]. V současné době vzhledem k situaci v okolních státech roste v ČR také obava z možných teroristických útoků, proto posílení jakéhokoli zabezpečení, a to včetně kontroly přístupu, vede k vyššímu zajištění fyzické bezpečnosti žáků, studentů. A to nejen před obavami z terorismu, ale také před jinými událostmi jako např. tragické události ze dne 14. 10. 2014 ve Žďáře nad Sázavou, kdy psychicky nemocná žena vnikla do budovy školy a napadla studenta, který následkům zranění podlehl. Volba vhodných opatření vedoucích ke zvýšení bezpečí studentů je náročná a není jednoduché vytvořit univerzální standard pro všechny školy. Standard by měl být obecným popisem. Tak je možno modifikovat řešení bezpečnostních opatření podle potřeb konkrétní situace na základě bezpečnostní analýzy pro konkrétní školu [3]. Nejen na základě uvedené události bylo dne 20. února 2015, pod č.j.MSMT-1981/2015-1, vydáno „Metodické doporučení k bezpečnosti dětí, žáků a studentů ve školách a školských zařízeních“ jako „Minimální standard bezpeč-

nosti“ 3]. Toto doporučení lze považovat za součást vyhlášky, která bude předpisem zákona 561/2004Sb. podle § 29 [3].

### **1.1 Elektronické zabezpečovací systémy – SKV, PZTS, CCTV**

Elektronické zabezpečovací systémy je skupina všech elektrotechnických prvků a komponent, které svojí funkcí zajišťují včasnou detekci, přesnou evidenci a přispívají k identifikaci narušitele. Do této skupiny patří: PZTS – Poplachové zabezpečovací a tísňové systémy, ACS - systémy kontroly vstupu, CCTV – uzavřený televizní okruh, a další systémy např. klíčové hospodářství, dorozumívací a komunikační systémy, systémy evakuačních, místních rozhlasů. V dnešní době existuje mnoho výrobců a ještě více dodavatelů v oblasti bezpečnostních technologií a to nejen z České Republiky. Nabízejí nepřehledné množství různých systémů jak od zahraničních, tak od českých výrobců. Pro zabezpečení školních objektů nebo kontrolu průchodu školních objektů nejsou specializované žádné bezpečnostní systémy ani CCTV systémy. Vzhledem k technickým a v dnešní době zejména softwarovým vybavením jednotlivých systémů lze úspěšně vybrat takový, který bude splňovat nejen všechny požadavky investora, ale také technické a legislativní předpisy pro Českou republiku

V této práci se podrobněji věnuji Elektronickým systémům kontroly vstupu v návaznosti na PZTS a CCTV.

### **1.2 Elektronické systémy kontroly vstupu**

Přístupový systém (ACS) nebo systém kontroly vstupu (SKV) v bezpečnostních aplikacích lze popsat jako soubor opatření vedoucí k zajištění řízení a evidence přístupu do zabezpečeného objektu nebo prostoru na základě jednoznačně přidělených přístupových práv. Opatření mohou být organizační (v úvodu zmíněné provozní řády), fyzické (ostraha), mechanické (zámky, mříže, trezory) nebo elektronické. Pro dosažení nejúčinnějšího zabezpečení je nejlepší kombinace všech opatření [4]. Elektronický systém kontroly vstupu je technické zařízení skládající se z libovolného počtu vzájemně propojených komponent. Úkolem systému je elektronická identifikace entity. Následné zpracování získaných dat probíhá v řídicí jednotce systému. Srovnáním s daty uloženými v systémové paměti a na základě předem stanovených přístupových práv, systém automaticky povolí/nepovolí ovládní přístupového místa. Jestliže část elektronického systému kontroly vstupu (např. roz-

hraní místa přístupu) tvoří část poplachového systému (narušení, tíseň) musí tato část splňovat požadavky příslušných norem [5].

Zjednodušeně lze říci, že základní funkcí elektronického systému kontroly vstupu je určení a zajištění *kdo* může *kam* a *kdy* vstoupit v rámci prostor chráněných tímto systémem. Jedná se tedy o restriktivní systém, který nesmí vpustit do chráněných prostor osobu bez oprávnění. Oproti klasickým mechanickým restriktivním systémům (klíče, zámky), které také brání v přístupu neoprávněných osob, mají SKV přesnou evidenci *kdo*, *kdy*, *kam*. Případně lze ztracený identifikační prvek jednoduše zneplatnit. U mechanických systémů nelze nastavit další podmínky přístupu, zatímco u SKV je to možné např. přidáním požadavku na zadání PINu, nebo zákaz opakovaného vstupu. Elektronické systémy mohou být propojeny s dalšími bezpečnostními systémy např. PZTS, CCTV, docházkovým systémem [6].

### 1.2.1 Terminologie SKV

- Elektronický systém kontroly vstupu – poskytuje oprávněným osobám, nebo entitám, vstup do nebo opuštění zabezpečeného prostoru, a zamítá vstup nebo odchod neoprávněným jedincům, nebo entitám.
- Řídící jednotka kontroly vstupu – část systému kontroly vstup, která je propojena se čtečkami, uzamykacími zařízeními a snímači rozhodující o poskytnutí nebo zamítnutí přístupu vstupním místem.
- Čtečka – zařízení pro čtení ověření.
- Přístup – akce vstupu dovnitř a výstupu ze zabezpečeného prostoru.
- Místo přístupu – fyzický vstup/výstup, v němž je přístup ovládán dveřmi, turniketem nebo jinou zabezpečovací závorou.
- Rozhraní místa přístupu – zařízení nebo obvod ovládající uvolnění a zajišťující místo přístupu.
- Přístupová úroveň – soubor pravidel užívaných k rozhodnutí, kde a kdy identifikační prvek poskytuje oprávněný přístup do jednoho nebo více přístupových míst. Může obsahovat zvláštní podmínky, jako např. povolený časový interval otevření určitého vstupního místa.
- Karta – typ identifikačního prostředku.
- Oprávnění – informace buď zapamatovaná, nebo uložená v identifikačním prostředku.
- Entita – jakýkoli pohyblivý objekt, kterému jsou poskytnuta práva přístupu.

- Událost – změna, nastávající v rámci elektronického systému kontroly vstupu.
- Elektromagnetický zámek/otevírač – elektricky ovládaný zámek/otevírač, který uzamyká/otevívá aktivací nebo deaktivací elektromagnetu, magneticky vázaného západkou.
- Biometrie – jakákoli měřitelná jedinečná fyziologická charakteristika nebo osobní rys sloužící jako identifikační prostředek k identifikaci a ověření jedince.
- Zábрана opakovanému průchodu – (anti – passback) pracovní režim který vyžaduje potvrzení uživatele při opouštění zabezpečeného a ovládaného prostoru za účelem nového vstupu a naopak.
- Autonomní režim – režim provozu elektronického systému kontroly vstupu bez komunikace mezi řídicí jednotkou a monitorujícím zařízením.
- Radiofrekvenční identifikační zařízení – bezkontaktní zařízení pro vysílání a/nebo příjem ověřovacích informací prostřednictvím radiových vln [5].

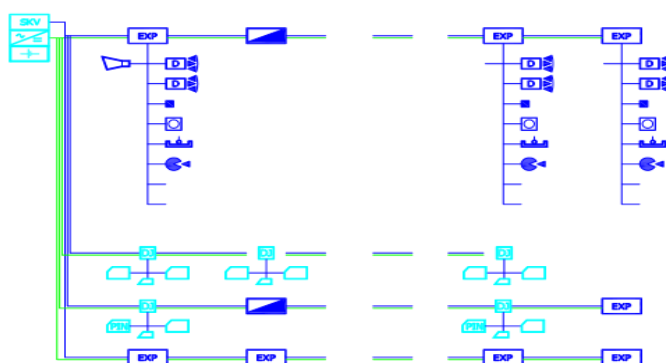
### 1.2.2 Topologie

Jedním ze základních rozdělení elektronických systémů kontroly vstupu je podle typu topologie systému.

- Autonomní systémy – obecně jde o nejjednodušší elektronický systém kontroly vstupu. Je tvořen max. 2 čtecími zařízeními, které jsou zároveň svými dveřními kontroléry, nastavení probíhá po vstupu do programovacího režimu a je ukládáno do paměti kontroléru. Další možností je systém s oddělenou, samostatnou dveřní jednotkou také pro připojení max. 2 identifikačních zařízení (vstup/výstup), které jsou připojeny např. sériovou linkou nebo komunikační sběrnici RS485. Dveřní jednotka v různých modifikacích umožňuje základní funkce jako: uvolnění/ blokace dveřních otevíračů, připojení odchodových tlačítek, signalizace nestandardních stavů dveří, přemostění, odblokování střežené oblasti systému PZTS. Napájení je řešeno inteligentními zdroji umístěnými v chráněné části. Nastavení přístupových práv probíhá v programovacím režimu každé dveřní jednotky a je ukládáno do interní paměti. Připojení řídicího PC slouží pro servisní programování nebo stažení historie událostí. Autonomní systémy jsou vhodné pro samostatné prostupy s menším počtem průchodů, nelze u nich provádět jednotnou nebo dálkovou správu uživatelů [4].
- Modulární systémy – jde o zařízení rozšiřitelné systémovými prvky až do naplnění HW možností systému. Jsou vhodné pro použití v rozsáhlých aplikacích. Základem systému

je řídicí jednotka nebo PC ve kterém probíhá ověření přístupových práv, časových závislostí atd. S ostatními komponenty, dveřními jednotkami (kontrolery) je propojená sběrníkovou nebo hvězdicovou topologií. Pokud se jedná o sběrníkovou topologii, pak jsou všechna přístupová místa propojena sběrníci (nejčastěji) typu RS485/422. Propojení přístupových míst hvězdicovou topologií je řešeno ethernetovou sítí [4]. Sběrníkově propojené jednotky přístupových míst jsou propojeny sběrníci RS485 s hlavní řídicí jednotkou a např. prostřednictvím převodníku RS 485/ USB jsou připojeny k PC. Vzhledem k vysoké spolehlivosti sběrnice RS485 i na velké vzdálenosti (1200m). U zařízení s tímto typem komunikace (master-multislave), kdy slave nemají žádnou možnost, jak začít vysílat bez možné kolize a čekají na přidělené právo od master stanice hovoříme o centrálním přidělování (master se periodicky dotazuje všech slave stanic zda nemají data k odeslání) [7] může docházet k omezení rychlosti vzhledem k rozsáhlosti systému. Z tohoto důvodu se na komunikační linku RS485 připojuje 32 jednotek přístupových míst. Tak se zpoždění téměř neprojevuje. U vybraných systémů jsou jednotky přístupových míst vybaveny interní pamětí pro uložení přístupových práv a s řídicí jednotkou, PC komunikují jen v případě varovných situací nebo při konfiguraci systému. Jedním z dalších typů systému kontroly vstupu jsou systémy, kde komunikační sběrnice propojuje přímo identifikační zařízení (čtečky) a rozhodování o přístupových právech je v hlavní řídicí jednotce.

Obrázek 1 Sběrníková topologie



Zdroj: Autor

Podobným způsobem lze popsat systém kde tento typ čteček je prostřednictvím převodníku RS485/ LAN připojen k běžné ethernetové síti. K ethernetové síti můžeme také připojit systémy s IP jednotkami přístupových míst. Odpadá tak omezení rychlosti



na komunikační sběrnici RS485. Kontrolér na ethernetové struktuře může sám inicializovat spojení s řídicí jednotkou nebo PC [4]. U všech uvedených modulárních systémů lze hlavní řídicí jednotky prostřednictvím ethernetové sítě propojit a využívat tak všech jejich výhodných vlastností. Tím se navyšuje kapacita pro obsluhu počtu přístupových míst. Zároveň jsou kladeny nároky na kapacitu pamětí hlavních řídicích jednotek pro vytvoření databází uživatelů. Z těchto důvodů se u rozsáhlejších systémů kontroly vstupu využívá aplikačních a databázových SQL serverů (aplikační servery mohou být jako služba). Databáze uživatelů jsou uloženy na serveru a jednotliví klienti pracují s uživatelským rozhraním. Komunikace probíhá prostřednictvím sítě ethernet přes TCP/IP protokol.

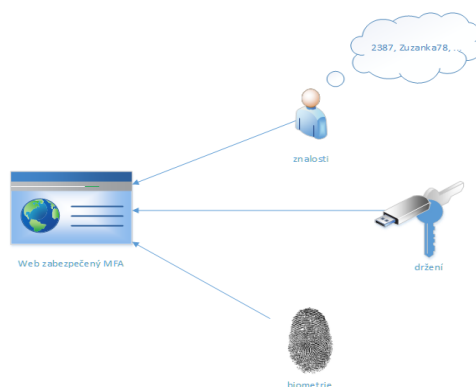
### 1.2.3 Identifikace

Z pohledu elektronického systému kontroly vstupu je identifikace proces, ve kterém prostřednictvím identifikačních prvků (identifikačního média identifikační karta s magnetickým páskem, identifikační karta s vlisovaným čipem, identifikační přívěšek, ale také otisk prstů, anatomie ruky, oční sítnice a duhovky apod.) dochází ke srovnání předem uložených dat v řídicí jednotce s daty získanými ze snímacích zařízení. Subjekt se může identifikovat těmito způsoby:

- Něco, co subjekt zná a co si pamatuje – heslo, kontrolní otázka.
- Něco, co má subjekt fyzicky u sebe – identifikační kartu, přívěšek.
- Sám sebou, nebo svými typickými rysy a chováním [4].

V případě požadavku na více identifikačních prvků se jedná o MFA (Multi Factor Authentication) vícefaktorová autentizace. Nejčastěji heslo + nějaký nezávislý identifikátor. Na identifikaci navazuje autorizace, která určuje, zda má uživatel povolen přístup k požadované službě. Pokud ano, je jeho požadavku o přístup vyhověno. Popsaný princip platí také pro automatizované komunikační systémy.

Obrázek 2 MFA Vícefaktorová autentizace



Zdroj:[8]

### 1.2.4 Role

Autentizační, identifikační prvky každého studenta, zaměstnance musí být různé, mohou se lišit i přístupová práva k požadovaným aplikacím nebo službám. Ve většině organizací ale existují skupiny pracovníků a nejen pracovníků, u kterých jsou přístupová práva stejná. V systému kontroly vstupu jsou zavedeny tzv. role. Jsou to předem vytvořené skupiny přístupových práv reprezentující např. skupiny zaměstnanců. ROLE, skupiny přístupových práv musí vždy respektovat bezpečnostní politiku organizace. Musí dodržovat pravidlo, že uživatel bude mít k dispozici jen minimální množství přístupových oprávnění, které ke své pracovní činnosti potřebuje.

Tabulka 1 Role

	ROLE 1	ROLE 2	ROLE 3	ROLE 4
	Manager 1 osoba	Pokladní 5 osob	Vědecký pracovník 4 osoby	Servis údržba 7 osob
Veřejné prostory				
Kanceláře				
Pokladny				
Laboratoře				
Badatelny				
Depozitáře				
Dílny				



povolený přístup

Zdroj: Autor

Závislosti mezi uživatelem a příslušnými rolemi, jsou neustále aktualizovány, díky systému IDM, který v pravidelných intervalech provádí ověřování přidělených práv [9].

### 1.2.5 Identifikační prvky

Identifikační prvek, ve vztahu k elektronickým systémům kontroly vstupu musí být jednoznačně přiřazen konkrétní osobě. Typ nosiče identifikační informace musí být v souladu se snímacím zařízením, důležitým ohledem při volbě přenosového média je bezpečnost uložené informace, kapacita pro uložení informace, mechanická odolnost. Podle principu činnosti dělíme identifikační prvky na:

**Manuální** - vyžadují manuální vstup od obsluhy, např. kódové zámky [4]. Pro uložení jednoznačné identifikační informace se využívá paměti osoby. Tato informace je prostřednictvím hardwarové klávesnice předána elektronickému systému kontroly vstupu jako osobní identifikační číslo PIN (personal identification number). PIN má přidělen každá osoba s povolenými přístupovými právy. Díky tomu lze z historie událostí systému zkontrolovat jednotlivé průchody. PIN má zadána skupina osob např. pro bytový dům, nelze určit průchod konkrétní osoby.

#### Čipové

Kontaktní, dotykové snímací zařízení je v přímém kontaktu s identifikačním prvkem, je možné čtení i zápis dat z kontaktních čipových karet. Paměťový čip o velikosti přibližně jeden čtvereční centimetr, je zalisován do nějakého mechanického nosiče, zpravidla plastové karty z PVC nebo ABS standardizovaných rozměrů dle ISO 7816. Bezpečnost karty je zajištěna její konstrukcí. Identifikační informace mohou být z mikročipu přečteny až při komunikaci s operačním systémem a navíc mohou být chráněny uživatelským heslem [4]. Dalším nosičem identifikační informace pro dotykové snímače je magnetická karta. Magnetická karta je identifikační plastová karta z PVC nebo ABS standartních rozměrů s pruhem citlivým na magnetické pole. Tento proužek slouží k uložení elektronické informace pomocí polarizovaných magnetických částic, je možné čtení i zápis dat. Bezpečnost a trvanlivost uložených dat je dána koercivitou magnetického materiálu. Nevýhodou je náchylnost na jakékoli magnetické pole případně mechanické poškození [10]. Oba typy identifikačních prvků se často vzájemně kombinují.

Bezkontaktní, bezdotykové snímací zařízení zpracuje vstupní informaci ve vzdálenosti několika centimetrů až metrů, je možné čtení i zápis dat.

- Radiofrekvenční identifikační prvky

Princip bezdotykového přenosu identifikačních údajů mezi identifikačním prvkem a snímacím zařízením je založen na radiofrekvenčním přenosu informace RFID. Základními prvky RFID systémů je řídicí PC, software pracující s databázemi uživatelů čtecí zařízení RFID reader (čtečka) s vysílací/přijímací anténou a tzv. RFID tag. RFID tagy lze rozdělit podle technického provedení aktivní, pasivní, použitých radiových frekvencí nebo použité paměti. Princip činnosti těchto systémů je založen na šíření elektromagnetických vln ze čtecího zařízení na nosném kmitočtu. Je-li v dostatečné vzdálenosti od vysílací antény tag naladěný na stejnou frekvenci je tato vlna přijata anténou tagu. Indukované napětí v tagu vyvolá střídavý elektrický proud, ten je usměrněn a napětí nabíjí kondenzátor v tagu. Po dosažení potřebné úrovně jsou spuštěny obvody v tagu a ten začne vysílat modulovanou odpověď.

#### Rozdělení tagů podle napájení

- pasivní, bez vlastního zdroje napájení. Je závislý na energii z antény čtečky, která šíří elektromagnetické pole. Omezená vzdálenost čtení podle použité frekvence a energetickém výkonu (desítky centimetrů až metr)
- aktivní, s vlastním zdrojem napájení. Tyto tagy nejsou závislé na čtecím zařízení. Lze použít pro monitorování pohybu osob, určení polohy v objektu. Schopnost čtení je až desítky metrů.

#### Rozdělení tagů podle frekvence

Kmitočet je nejdůležitější parametr který určuje dosah a rychlost čtení systému. Pro větší vzdálenost a rychlost čtení je nutno použít vyšších frekvencí. Nevýhodou vyšších frekvencí je vyšší citlivost na materiály které omezují šíření elektromagnetických vln (kovy, uhlík, kapalina). Pro systémy RFID jsou čtyři hlavní frekvenční pásma

- LF (Low Frequency) pásmo 125 -134 kHz podle ISO11784/5, ISO1422. velmi krátká čtecí vzdálenost (do cca. 20 cm) a nízká přenosová rychlost. Použití u pasivních tagů, které se skládají z kotouče měděného drátku a většinou nepřepisovatelné paměti RO(read only)
- HF (High Frequency) pásmo 13,56 MHz podle ISO15693,ISO14443. pásmo s vyšší čtecí vzdáleností (do cca. 1 metru). Poskytuje vyšší pře-

nosovou rychlost a spolehlivost v blízkosti zejména kovů. Anténa tagu je vyrobena z měděného drátu nebo vytištěna vodivým inkoustem na papírovou podložku a doplněná čipem RO nebo RW(read write) s kapacitou většinou 1- 4kb.

- UHF (Ultra High Frequency) pásmo 860 - 960 MHz) podle (EPC Electronic Product Code, jednotný číselný standard). pásmo pro přenos informace na vzdálenosti jednotek metrů, využívá standard ISO 18000 určený pro knihovny a docházkové systémy
- MW (Microwave) pásmo 2,45, až 8 GHz - MW velká čtecí vzdálenost a vysoká přenosová rychlost, velmi citlivé na rušení v přítomnosti kovu a tekutin. Pracuje v blízkosti frekvenčního pásma často používaných Wi-Fi sítí s aktivními tagy, s vlastním zdrojem energie. Použití např. pro identifikaci vozidel a pohybujících se předmětů (Real Time Location Services) [11].
- Optické identifikační prvky jsou dalším typem bezkontaktní identifikace. Do této skupiny patří všechny typy čárových kódů, kódy kruhové, QR kódy. Princip čárového je založen na absorpci IR paprsku u černých čar a odrazu IR paprsku od bílých mezer. Fotocitlivý prvek (senzor) odražené světlo přijímá a převede na elektrický signál. Ten je dále zpracován dekodérem a data jsou odeslána do PC k vyhodnocení. Obsahem každého čárového kódu je takzvaný start znak, zadaná informace, kontrolní součet a stop znak. Mezi nejužívanější je 8 nebo 13 místní kód EAN. Provedení čárových kódů je nekryté nebo maskované, ty jsou zapouzdřené v PVC folii s ochranou maskovací vrstvou, nebo pod vrstvou maskovacího laku který IR světlo. Nevýhodou čárových kódů je, velmi snadné zneužití [12].
- Biometrické identifikační prvky jsou skupina prvků zahrnující prvky, které obsahují biometrické rysy. Jako identifikační znaky se u těchto zařízení využívá některých částí lidského těla. Odpadá tak použití externích paměťových identifikačních prvků. V současné době se jedná o nejbezpečnější identifikační systémy. Rozpoznávací znaky jsou jedinečné pro každou osobu, biometrické znaky se nemění s časem, snímání není náročné. Nevýhodou je prozatím stále vysoká pořizovací cena těchto snímacích zařízení. Vzhledem k velikosti porovnávaných dat často také rychlost odezvy řídicích systémů. Hlavně z tohoto důvodu se v praxi u biometrických systémů setkáváme s metodou „1:N“ nebo „1:1“. První ze jmenovaných metod porovnává

v celé databázi uložených identit. U druhé metody je požadován další identifikační stupeň, systém potom kontroluje jen přihlášeného uživatele. Nejrozšířenější biometrické systémy využívají biometrických znaků otisku prstu nebo geometrie prstu nebo ruky. Existují biometrické snímací prvky, které využívají pro verifikaci přístupu oční sítnice a duhovky, charakteristické rysy obličeje, rozpoznání lidského hlasu, způsob podpisu, krevního řečiště apod. [4].

- Otisk prstu

Rozpoznání podle otisku prstu je dnes jedním z nejznámějších, nejdostupnějších a nejrychlejších způsobů biometrické identifikace. Identifikace podle otisku prstu se řadí do skupiny daktyloskopických identifikací. Podle uloženého vzorku otisku umožňují velmi rychlou identifikaci oprávněné osoby a uvolnění přístupu. Existuje několik metod jak zachytit otisk prstu. Jedním z nich je klasická metoda pomocí papíru a inkoustu (pro forenzní oblast). Nejběžnější metoda je tzv. statické snímání, kdy prst bez pohybování nebo tlaku přiložíme k senzoru. Další metoda je tzv. šablonováním, kdy prst přejíždí přes úzký křemíkový senzor. Výsledný obraz skládá z načtených pásů [13].

- Geometrie ruky

Metoda identifikace podle geometrie (morfologie) ruky je založena na principu měření a 3D snímání povrchu ruky včetně zjištění délky, šířky, tloušťky. Měření probíhá pomocí CCD kamery na speciální podložce s pěti polohovými kolíky. Použití v docházkových systémech [13].

- Oční duhovka a sítnice

Metoda identifikace podle oční duhovky je jedna z nejpresnějších, nejrychlejších a z hlediska bezpečnosti nejbezpečnějších metod. Tato metoda má nejvíce identifikačních možností, nelze nalézt dvě stejné oční duhovky ani u jednoho člověka. Během snímání duhovky vznikají fázorové diagramy, které obsahují informaci o pozici individuálních plošek, jejich četnosti a orientaci. Pro identifikaci pak slouží duhovkové mapy, které vznikají ze získaných informací. Pro snímání duhovky je nezbytná velmi kvalitní digitální kamera. Identifikace osoby podle sítnice se považuje za velmi přesnou metodu, její použití je pro oblast nejvyššího stupně zabezpečení. Pro získání obrazu struktury cév na pozadí lidského oka se používá zdroj světla s nízkou intenzitou záření a opto-elektrický systém [13].

### 1.2.6 Snímací zařízení

Snímací zařízení je členěno do skupin jednak podle použitého identifikačního média jak je uvedeno dříve a jednak podle dostupných funkcí daného zařízení. Členění vzhledem k vlastnostem:

- Základní – nejčastěji používané snímací zařízení. Zjistí čísla identifikátoru, zajistí vzorky biometrických údajů a zprostředkuje předání k nadřazené dveřní jednotce. Komunikace probíhá prostřednictvím komunikačních protokolů např. ABA nebo Wiegand v různých bitových délkách 26, 32, 56. Monitorování vstupních informací a ovládání výstupních zařízení je prostřednictvím dveřních jednotek. Rozhodovací činnost probíhá až v řídicí jednotce, ke které jsou dveřní jednotky připojeny komunikační sběrnici, nejčastěji RS 485.
- Poloautonomní – tento typ snímacích zařízení zajistí navíc také informace o vstupních a výstupních zařízeních. Jejich součástí jsou monitorovací vstupy pro kontrolu např. stále otevřených dveří. Jejich součástí jsou také ovládací výstupy na uvolnění dveřních otvíračů. S řídicí jednotkou, ke které jsou připojeny komunikační sběrnici např. RS 485, ověřují pouze umožnění přístupu.
- Autonomní – snímací zařízení v této skupině jsou vybaveny všemi potřebnými vstupy a výstupy pro monitorování a ovládání. Zajišťují také plnohodnotné rozhodovací činnosti v oblasti povolení /zakázání přístupu. Pokud jsou připojeny k řídicí jednotce, tak pro předání informací o proběhlých událostech případně pro zajištění aktualizace přístupových práv. Komunikace probíhá prostřednictvím linek RS 485, nebo dnes již častěji LAN. V tomto případě hovoříme o IP čtečkách [4].

### 1.2.7 Ovládaná zařízení

Každý systém kontroly vstupu je určen k řízení prostupů, ve svých jednotkách je vybaven vstupními a výstupními kontakty pro monitorování a ovládání připojených zařízení. Mezi nejčastěji používaná ovládaná zařízení patří elektromagnetické otvírače v provedení běžném (fail secure bez připojeného napětí stále uzavřeno) nebo reverzním (fail safe bez připojeného napětí uvolněno), jsou instalovány do zárubní dveří. Dále elektromechanické samozamykací zámky, elektromotorické zámky, kdy po uzavření dveří je mechanicky/elektricky vysunuta závora zámku, nebo přídržné elektromagnety. Nejčastější použití je na skleněných dveřích. Ovládaná zařízení jsou vždy použita podle konkrétní situace a potřeb každé aplikace [4].

### 1.3 Poplachové zabezpečovací a tísňové systémy PZTS

Poplachový zabezpečovací a tísňový systém je soubor technických prostředků, ústředny, detektorů, tísňových hlásičů, technických podpůrných prostředků, prvků poplachové signalizace, přenosových zařízení, ovládacích zařízení, jejichž prostřednictvím je opticky nebo akusticky signalizováno na určeném místě narušení chráněného objektu [14]. Je to zařízení, které slouží k včasné signalizaci přesného místa narušení. Systém umožňuje předání poplachové informace na zvolená místa, čímž usnadní činnost zásahové služby. Systém podporuje fyzickou ochranu objektu a doplňuje ochranu mechanickými zábrannými prostředky. Dotváří kombinaci bezpečnostních opatření a spolu s provozními řády zvyšuje celkové zabezpečení objektů nebo areálů [12]. Systém PZTS se skládá z těchto základních částí:

- Ústředna systému – řídí celý systém, je naprogramována tak aby dokázala řídit celý systém autonomně, přijímat povely obsluhy a předávat informace o stavech systému.
- Ovládací prvky systému - jedná se systémové ovládací klávesnice nebo integrační a nastavbové systémy.
- Systémové linkové moduly – slouží pro připojení detektorů různých typů do systému.
- Detektory - jedná se o prvky poskytující systému informace o narušení.
- Napájecí zdroje – Hlavní napájecí zdroje, záložní napájecí zdroje, poskytují systému napájecí napětí všech komponent s dostatečnou kapacitou i v případě výpadku elektrické energie.

Základní členění systému PZTS je definováno podle typu ochrany:

- Plášťová ochrana – ochrana obvodu budovy nebo areálu.
- Prostorová ochrana – ochrana vybraných prostor budovy detektory pohybu.
- Komplexní ochrana – kombinace prostorové a plášťové ochrany [15].

#### 1.3.1 Terminologie

dle ČSN EN 50131-1 ed.2 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – část 1 – Systémové požadavky:



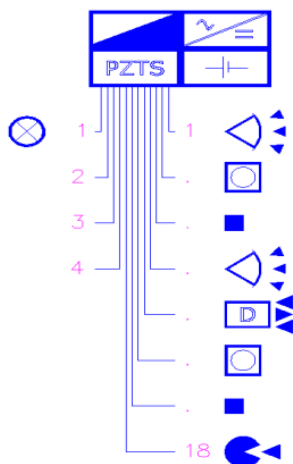
- Poplachové přijímací centrum – Trvale obsluhované dohledové pracoviště (ARC) do kterého jsou předány informace týkající se stavu jednoho nebo více I&HAS.
- Poplachové přenosové systémy – Zařízení a síť používané pro přenos informací, týkajících se stavů jednoho nebo více I&HAS do jednoho nebo více ARC.
- Komunikace – Přenos signálů anebo zpráv mezi komponenty. Může se jednat o kontakty spínacího prvku, kterými prochází stálý elektrický proud.
- Ústředna – Zařízení pro příjem, zpracování, ovládání, indikaci a iniciaci následného přenosu informace.
- Událost - stav vyplývající z provozu I&HAS, např. aktivace střežení, přechod do klidu, poplachový stav.
- Indikace – informace (akustická, optická nebo jakákoli další) usnadňující uživateli obsluhu I&HAS.
- Poplachový zabezpečovací a tísňový systém – kombinovaný systém určený k detekci poplachu vniknutí a tísňového poplachu.
- Odpojení (přemostění) – zásah uživatele, povolující uvést zařízení do stavu střežení v případě výskytu poruchového stavu.
- Sabotáž, Detekce sabotáže – Úmyslný zásah nebo nedovolené manipulování s I&HAS nebo jejich částí a jejich rozpoznání, detekce [16].

### 1.3.2 Topologie

Základní členění systémů PZTS je možné podle typu komunikace a počtu připojitelných detektorů k ústředně.

- Drátové smyčky připojené přímo k ústředně – tento typ systémů je nejčastěji využíván pro objekty malého až středního rozsahu s využitím zónového nebo ATZ zapojení smyček.

Obrázek 3 PZTS Drátové prvky - PZTS Ústředna



Zdroj: Autor

- Drátové smyčky připojené k rozšiřujícím modulům - moduly předávají informace o stavech detektorů do nadřazené ústředny prostřednictvím komunikační sběrnice RS 485. Zapojení smyček je nejčastěji dvojité vyvážené pro každý detektor. Sběrnice systémy jsou pro svoji modularitu nejčastěji využívány pro rozsáhlé systémy. Na komunikační sběrnici připojujeme nejčastěji 30 -32 komunikačních modulů. Podle technické vybavenosti ústředny můžeme sběrnice systémy propojovat prostřednictvím Ethenetu a vytvářet rozsáhlé systémy s jednotnou správou systému.
- Bezdrátové spojení – komunikace probíhá prostřednictvím radiového modulu, který je součástí každého detektoru a ústředny. Šifrovaná komunikace probíhá v pásmu 868MHz. U rozsáhlých aplikací lze využít v kombinaci s radiovými linkovými moduly, které jsou připojeny s drátovými systémy. Komunikace od koncových prvků k nadřazenému probíhá tak, že v pravidelných časových intervalech koncový prvek odešle informaci o svém stavu – tzv. jednosměrná komunikace. Pro vyšší stupně zabezpečení využijeme systémy podporující obousměrnou komunikaci, kdy nadřazené prvky se dotazují a na stav konkrétního detektoru přímo, anebo prostřednictvím radiové sítě a radiových modulů (směrování) [4].

### 1.3.3 Detektory

Jsou technické prostředky, které v oblasti bezpečnostního průmyslu nahrazují a zdokonalují lidské smysly a plně automaticky předávají informaci o stavech narušení nebo klidu. V oblasti bezpečnostních technologií rozdělujeme tyto prvky do skupin

- Prvky plášťové a prostorové ochrany
  - magnetické, mechanické kontakty, spínače
  - prostorové detektory mikrovlnné, infračervené, duální
  - mikrofonní detektory (ochrana skleněných ploch)
  - vibrační detektory
- Prvky předmětové ochrany
  - kapacitní detektory
  - tahové detektory
  - tenzometrické detektory
- Prvky perimetrické ochrany
  - IR a MW závory a bariéry
  - šterbinové kabely
  - tlakové detektory
  - seizmické detektory
- Prvky osobní ochrany
  - tísňové hlásiče – skryté, veřejné, osobní [4].

### 1.4 Integrace

Systém kontroly vstupu je jedna část z oblasti bezpečnostních technologií. Běžně se setkáváme s požadavkem na vzájemnou kombinaci bezpečnostních slaboproudých systémů zejména kombinaci na PZTS (zastřežení/odstřežení systému nebo subsystému), nebo kombinaci s CCTV (synchronizace se systémem CCTV, zobrazení procházející osoby), případně provázanost s dorozumívacím zařízením (spuštění audio hlášení pro navádění, nebo např. informace o poloze). Dále s provázaností se systémy elektrické požární signalizace, nouzového sdělovacího zařízení, nouzového naváděcího systému nebo nouzového osvětlení a to zejména pro usnadnění evakuace osob z objektu v případě mimořádné události. Popsané činnosti jsou často prováděny na úrovni hardwarových propojení. Další možností je integrace systémů kontroly vstupu přímo do řídicí jednotky systému PZTS a mít shodnou

databázi uživatelů pro oba systémy. U těchto systémů je možné monitorování průchodů osob v on-line režimu na některém připojeném klientském pracovišti.

Systém kontroly vstupu a jeho integraci lze řešit také na úrovni další softwarové integrace. Jedná se o nadstavbové grafické systémy, tyto systémy pak přinášejí obsluhu jednotné grafické pracovní rozhraní pro monitorování mnoha technologií s jejich vizualizací. Tato řešení jsou vhodná pro rozsáhlé aplikace s mnoha různými technologiemi. U SW integrací se nejčastěji využívají technologie server - klient s přístupem do SQL databází uživatelů. Databáze uživatelů poskytují informační systémy společností ze svého Identity managementu. K databázím uživatelů pak systémy přistupují prostřednictvím komunikačních protokolů, nejčastěji LDAP a vzájemném ověření.

## 1.5 Identity management

### 1.5.1 Definice

Identity management je definován několika možnými způsoby, předkládám některé konkrétní:

Identity Management - vytvoření flexibilních definic pro jednotlivce i skupiny, které ověřují uživatele a umožňují různé úrovně oprávnění v závislosti na využívané službě [17].

Správa identit (správa ID) je široká administrativní oblast, která se zabývá identifikací jednotlivce v systému (jako jsou například země, síť nebo společnosti) a kontroly jejich přístupu ke zdrojům v rámci těchto systémů tím, že se sdruží uživatelská práva a omezení k zavedené identitě [18].

Z uvedených definic je zřejmé, že Identity management se zabývá vznikem a správou elektronických identit a přiřazování příslušných oprávnění k uživatelskému účtu. Je také zřejmé, že v současné době je Identity management (IDM) základní stavební prvek většiny společností nebo organizací. Ve většině organizací je přirozenou součástí každodenních činností většiny zaměstnanců v kancelářích nebo ve výrobním procesu. Současné moderní systémy pro správu uživatelských rolí a práv nabízí řadu funkcí s přidanou hodnotou, které se pozitivně projevují na příklad ve zvýšení produktivity nebo zajišťování lepšího zabezpečení přístupu k firemním systémům ICT.

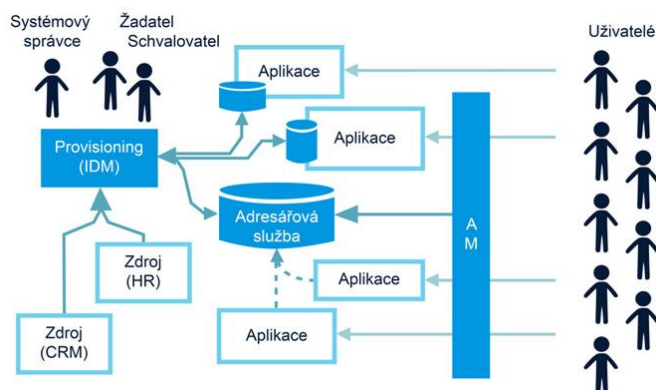
Společnosti obecně využívají celou řadu různých aplikací a systémů s různou vzájemnou závislostí. V prostředí, které soustřeďuje několik systémů nebo aplikací, pak stojí před

problémem jak přehledně evidovat přístupy k jednotlivým systémům, evidovat změny v uživatelských oprávněních a přidělovat role v aplikacích pro fungování společnosti či výrobních systémech nebo aplikacích. Příchod nového zaměstnance, nebo naopak ukončení zaměstnání znamená pro systémy vznik tzv. životního cyklu entity. Vznikají tak ve většině případů přístupy ke koncovým pracovním stanicím, elektronické poště, intranetu. V průběhu doby přibývá oprávnění a následuje nelehký úkol v nastavení jednotlivých aplikací, systémů a udržení přehledu o jeho změnách, využití či zneužívání. Identity management je tedy informační systém, díky kterému umíme obsluhovat z jednoho místa životní cykly uživatelských účtů. Přehledně jsou k dispozici informace, jakými účty uživatel disponuje a jaká má oprávnění. Je možné jednoduše provádět kontrolní audity. Identity management díky automatickým procesům např. automatická synchronizace identit, může přinášet také snížení nákladů na lidskou obsluhu [9].

### 1.5.2 Architektura

Nejběžnější řešení architektury systému identity managementu je takové, kdy jednotlivé koncové aplikace, či systémy jsou centrálně orientované. Všechny koncové prvky mají vlastní úložiště uživatelských účtů a jsou napojeny prostřednictvím tzv. konektorů. V současné době se využívá standartních komunikačních protokolů jako např. JDBC, SSH, LDAP atd. Výhodou oproti klasickému způsobu je absence nutnosti přizpůsobovat koncový prvek pro identity management. Princip Identity managementu je tedy poskytnutí potřebných dat do koncových prvků na základě autoritativní informace a koncové prvky proti svému úložišti řídí autentizaci a autorizaci uživatele. Pro Access management platí, že jednotlivé koncové prvky se dotazují a ověřují možný přístup k centrální jednotce identity managementu [9].

Obrázek 4 Architektura IDM



Zdroj: [19]

Access management je tedy porovnání aktuální žádosti uživatele o přístup k informačnímu systému. Tento proces probíhá prostřednictvím nástroje např. Access Manager, ten v reálném čase vyhodnocuje oprávněnost požadavku. Běžně se obě architektury kombinují a setkáváme se tak s Identity a Access managementem [8]. Jedním z možných řešení je tedy portál interních identit, ten dovoluje integraci jednotlivých firemních systémů. Dalšími články takového řešení pak jsou aplikační protokoly, např. LDAP s adresářovou službou Active Directory a personální informační systémy, z nichž jsou čerpána kmenová data o všech uživateli [20].

### 1.5.3 SSL (Secure sockets Layer) a TLS (Transport Layer Security)

V rámci identity managementu se pro správu případně servis často využívá vzdáleného přístupu k serverům prostřednictvím TCP/IP. V této situaci se pro zvýšení zabezpečení datových přenosů a autentizaci využívá šifrování přenášených dat. Šifrování zajišťují certifikované protokoly. Jedním z nejrozšířenějších protokolů v rámci internetu mezi serverem a webovým prohlížečem je SSL. Jedná se o internetovský protokol, v síti nad transportním spojením zajišťuje důvěrnost, autenticitu, originalitu a integritu dat mezi klientem a serverem. Jeho následníkem je pak TLS (vychází z verze SSL 3.0). Je sestaven ze dvou částí, TLS Handshake Protokol pro vzájemnou autentizaci a ustanovení kryptografického algoritmu a TLS Record Protokol pro zajištění požadované úrovně bezpečnosti podle dohodnutého algoritmu (např. DES). Nastavení spojení je tedy založeno na asymetrickém šifrování a dvou šifrovacími klíči, veřejným, soukromým a na nastavení šifrované komunikace. Nastavení probíhá v několika krocích.

- Klient pošle požadavek na šifrované spojení (připojení ze zabezpečeného portu) spolu s dalšími informacemi (jaké algoritmy budou použity).
- Server odešle odpověď na požadavek spolu s certifikátem.
- Klient podle přijatého certifikátu ověří autentičnost serveru a spolu s certifikátem obdrží veřejný klíč serveru.
- Díky obdrženým informacím klient vygeneruje základ šifrovacího klíče, kterým se bude šifrovat další komunikace, zašifruje ho veřejným klíčem serveru a odešle.
- Server svým soukromým klíčem rozšifruje základ šifrovacího klíče a oba z tohoto základu vygenerují hlavní šifrovací klíč.
- Navzájem si potvrdí komunikaci tímto šifrovacím klíčem [21].

Obrázek 5 SSL/TLS komunikace



Zdroj:[21]

## 2 LEGISLATIVA

„Technické normy jsou předpokladem technického pořádku v daném oboru na příslušné úrovni“ [14]. Nejen pro bezpečnostní technologie vznikl v Evropě Evropský výbor pro normalizaci v elektrotechnice (CENELEC), ve světě pak Mezinárodní výbor pro elektrotechniku (IEC). V České republice je centrálním orgánem pro normalizaci od roku 2008 Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (UNMZ). „Legislativní základ oboru je tvořen Zákonem č. 102/2001 Sb. Obecná bezpečnost výrobku dále Zákonem č. 22/97 Sb. o technických požadavcích na výrobky ve znění pozdějších předpisů. Tento zákon byl schválen 24. 1. 1997 a nabyl účinnosti v 1. 9. 1997“ [14]. Přijetím tohoto zákona plní Česká republika závazky vyplývající z asociační dohody s EU které byly uzavřeny v roce 1995.

Dále zákonem č. 59/199 Sb o odpovědnosti za škodu způsobenou vadou výrobku, zákonem č. 64/1986 Sb. o české obchodní inspekci [22]. Zákony stanovují výrobcům a dovozcům základní podmínky:

Na trh uvádět jen bezpečné výrobky, (takové, které za normálních podmínek nejsou nebezpečné při jejich používání). U ostatních, potenciálně nebezpečných, které jsou zmiňovány v příslušných nařízeních vlády, výrobci a dovozci musí:

- Dodržet vlastnosti výrobku požadované technickými předpisy, technickými normami. Přestože technické předpisy mají doporučující charakter, pokud je na ně odkazováno např. sbírkou zákonů, nařízením vlády, vyhláškou atd. je povinnost tyto technické předpisy dodržet.
- Posoudit shodu stanoveného výrobku podle postupu uvedeného v nařízení vlády.
- Vydat prohlášení o shodě ke každému výrobku podle náležitostí uvedených v nařízení vlády.
- Označit výrobek značkou shody. V současnosti lze v ČR označovat výrobky CE.

„V oboru zabezpečovací techniky a slaboproudých systémů jsou z pohledu zákona č. 22/97 Sb., o technických požadavcích na výrobky nejdůležitější nařízení vlády, jimiž se stanoví“:

- Technické požadavky na zařízení nízkého napětí LVD (NV č. 17/2003 Sb).



- Technické požadavky z hlediska elektromagnetické kompatibility EMC, (NV č. 616/2006 Sb). Elektromagnetická kompatibilita je schopnost zařízení včetně rozvodů být spolehlivě v provozu při vlivu elektromagnetického pole, a zároveň svým elektromagnetickým polem neovlivňovat ostatní zařízení nebo systémy [22].

Každá část v oboru bezpečnostních technologií se řídí svojí skupinou norem. Pro poplachové systémy platí řada norem EN 50130.

- EN 50130 + Všeobecně
- EN 50131 + PZTS
- EN 50132 + CCTV
- EN 50133 + ACS (platnost do 11. 6. 2016)
- EN 50134 + SAS systémy přivolání pomoci

Kromě norem EN 50130, EN 50137 je pro ostatní normy stejné členění, a to:

- ČSN EN 5013x-1            Systémové požadavky
- ČSN EN 5013x-y            Produktové normy (např. požadavky na detektory)
- ČSN EN 5013x-7            Aplikační směrnice

Pro vzájemnou integraci bezpečnostních technologií se řídíme dle ČSN CLC/TS50398 [22].

## 2.1 ACS - Systémy kontroly vstupu

Systémy kontroly vstupu se řadí stejně jako systémy PZTS do skupiny bezpečnostních systémů. Stejně také mají svoje legislativní předpisy. Přestože se v této oblasti neustále objevují nové prvky usnadňující zjednodušující a zrychlující např. čtení, porovnání vstupních informací s uloženými daty, nebo zrychlení komunikace mezi přístupovými body a řídicí jednotkou, Stejně pro systémy ACS stále platí základní pravidla uvedená normách řady EN 50133 :

- ČSN EN 50133-1 Poplachové systémy - Systémy kontroly vstupu pro použití v bezpečnostních aplikacích – část 1: Systémové požadavky

- ČSN EN 50133-2-1 Poplachové systémy - Systémy kontroly vstupu pro použití v bezpečnostních aplikacích – část 2-1: Všeobecné požadavky na komponenty
- ČSN EN 50133-7 Poplachové systémy - Systémy kontroly vstupu pro použití v bezpečnostních aplikacích – část 7: Pokyny pro aplikace
- ČSN EN 50130-4 ed.2 Poplachové systémy - část 4: Elektromagnetická kompatibilita
- ČSN EN 50130-5 ed.2 Poplachové systémy část 5: Metody zkoušek vlivu prostředí
- ČSN CLC/TS 50398 Poplachové systémy – Kombinované a integrované systémy – Všeobecné požadavky
- ČSN EN 60839-11-1 Poplachové a elektronické bezpečnostní systémy část 11-1: Elektronické systémy kontroly vstupu- požadavky na komponenty [23].

ČSN EN 50133-1 - platnost této normy končí 11. 6. 2016. Souběžně s touto normou platí od 02/2014 nová norma ČSN EN 60839-11-1. Dále uvedu nejvýznamnější rozdíl mezi oběma normami.

Podle ČSN EN 50133-1 je míra, klasifikace zabezpečení systému kontroly vstupu založena na klasifikaci identifikace a na klasifikaci přístupu, kdy tyto klasifikace můžeme definovat pro každé místo přístupu a to pro vstup a výstup odděleně. Je to nezávislá kombinace tříd identifikace a přístupu.

### 2.1.1 Třídy identifikace

- **Třída 0** – Není požadována identifikace, vstup je umožněn pomocí tlačítek. Oprávnění vstupu povoluje na základě kontroly průkazu (povolení ke vstupu) fyzická ostraha
- **Třída 1** – Nutnost zadání identifikační informace (PIN, apod.), zadaný údaj je porovnán s uloženými informacemi v paměti jednotky.
- **Třída 2** – Požadavek na použití identifikačního předmětu, např. karty RFID, nebo biometrie. Uživatel má přiřazenu digitální identitu, není možné vytvořit snadnou kopii identifikačního prvku pomocí lidského oka (zpozorovat PIN).
- **Třída 3** – Kombinace třídy 1 a třídy 2. Užití hesla, PIN u, a identifikačního prvku.

### 2.1.2 Třídy přístupu

- **Třída A** – Není požadováno uložení přístupových informací, bez časového omezení přístupu, (časové filtry)
- **Třída B** – Požadavek na užití časových filtrů a ukládání přístupových informací o stavu systému (neoprávněné otevření dveří apod.) [24].

Podle ČSN EN 60839-11-1 je stanovení úrovně ochrany systému kontroly vstupu a jeho komponent, včetně požadavku např. na monitorování a aktivaci přístupových míst, rozpoznávání, signalizaci nátlaku atd. ve vazbě ke stupňům rizika 1 – 4, podobně jakou PZTS.

- **Stupeň 1** – nízké riziko – (hotel, penzion)
- **Stupeň 2** – nízké až střední riziko (kanceláře, malá firma, škola)
- **Stupeň 3** – střední až vysoké riziko (finanční domy, průmysl)
- **Stupeň 4** – vysoké riziko (výzkum, vývoj, kritická infrastruktura, vládní, vojenské budovy)

Podobně jako v předešlé normě můžeme stanovit různé stupně včetně volitelných funkcí pro různá přístupová místa. V takovém případě je nutné tato místa v dokumentaci popsat.

Při návrhu technického řešení a následné realizace je nutné respektovat také požadavky uvedené v normách řady ČSN EN 33 2000 na elektrické instalace nízkého napětí např.:

- ČSN 33 2000-4-41 ed.2 Elektrické instalace nízkého napětí část 4-41: Ochranná opatření pro zajištění bezpečnosti – Ochrana před úrazem elektrickým proudem
- ČSN 33 2000-5-51 ed.3 Elektrické instalace nízkého napětí část 5-51: Výběr a stavba elektrických zařízení – Všeobecné předpisy
- ČSN 33 2000-6 Elektrické instalace nízkého napětí – část 6 : Revize

V systémech kontroly vstupu je nezbytné zejména při jejich návrhu brát v úvahu nejen požadavek na zvýšení zabezpečení objektu znemožněním vstupu nežádoucích osob, který požadován uvedenou normou, ale také požadavek na zajištění požární bezpečnosti v případě výjimečné situace, zejména v případě nutnosti evakuace osob [5].

### 2.1.3 Návrh systémů kontroly vstupu

Postup při návrhu systému kontroly vstupu vychází z ČSN EN 50133-7 pokyny pro aplikace a z doporučení výrobců. Jednou z nejdůležitějších etap při návrhu je zadání, podle kte-

rého celý systém navrhujeme. Zadání vychází z potřeb investora a jsou během konzultací upřesňována. Při návrhu dále postupujeme podle základní osnovy.

- Analyzujeme možná rizika v konkrétní lokalitě a určíme jejich min. a max. hranice.
- Zjistíme požadavky na bezpečnost provozu budoucího systému z hlediska nouzových a únikových východů včetně provozu pro tělesně postižené osoby.
- Zjistíme požadavky na konstrukci systému z hlediska vnějších a vnitřních vlivů prostředí.
- Zjistíme požadavky na třídy identifikace, předpokládaný počet uživatelů a jejich četnost průchodů, ovladatelnost systému, zálohu systému z hlediska napájení, z hlediska ukládání a obnovy dat a obnovy provozu.
- Zjistíme požadavky na systém z hlediska obsluhy vjezdů vozidel, správy knihy návštěv.
- Zjistíme požadavky na vazby mezi ostatní technologie, zařazení a zobrazení v integračních softwarech. Požadavky na poskytování koordinovaných hlášení.
- Zjistíme možnosti konstrukce objektu z hlediska možných kabelových tras.
- Dohodneme vhodné identifikační prvky, programování a správu systému.

Při konzultacích je investor seznámen s technickými možnostmi různých systémů. Výsledek konzultací vede k určení technických podmínek, technického řešení a stanovení vhodné technologie pro zpracování návrhu skladby systému. Dalšími kroky jsou zpracování projektové dokumentace systému kontroly vstupu, po jeho odsouhlasení pak instalace systému dle návodů na instalaci. Následuje předání systému do provozu. Probíhá podle předem stanovených dohod součástí je výchozí revizní zpráva, návody na provoz a údržbu, návrhy provozu, dokumentace skutečného stavu instalace systému, provozní kniha atd.. Před spuštěním systému do trvalého provozu jsou uživatelé seznámeni s ovládáním a běžnou údržbou systému. V tomto období lze stanovit tzv. zkušební provoz systému, při kterém probíhá monitorování bezproblémového chodu celého systému v reálných podmínkách provozu. Po jeho ukončení systém automaticky přechází do trvalého provozu [22].

Poplachové systémy – Poplachové zabezpečovací a tísňové systémy

Při návrhu a zřizování poplachového zabezpečovacího a tísňového systému se řídíme dle ČSN EN 50131-7 (část 7 Pokyny pro aplikace). Tento dokument je rozdělen do kapitol:

- Návrh systému
- Příprava realizace
- Realizace
- Kontrola, funkční zkouška, převímka
- Dokumentace a záznam provozu systému
- Provoz systému
- Údržba a opravy

Ve všech kapitolách je popsán doporučený postup prováděné činnosti. Dalším důležitým podkladem pro správný návrh systému PZTS jsou předem stanovené požadavky na stupeň zabezpečení a třídy prostředí [22].

Tabulka 2 Stupně zabezpečení PZTS

Stupeň 1	Nízké riziko	Předpokládá se, že pachatel má malou znalost PZTS a má k dispozici omezený sortiment dostupných nástrojů
Stupeň 2	Nízké až střední riziko	Předpokládá se, že pachatel má částečné znalosti se systémy PZTS a má k dispozici běžně používané nářadí
Stupeň 3	Střední až vysoké riziko	Předpokládá se, že pachatel je znalý systémů PZTS a má k dispozici velký sortiment nástrojů a elektronických zařízení
Stupeň 4	Vysoké riziko	Předpokládá se, že pachatel je schopen zpracovat plán vniknutí a má k dispozici kompletní soubor nástrojů a zařízení včetně komponentů systému určených pro náhradu části systému

Zdroj: [25]

Tabulka 3 Třídy prostředí

Třída prostředí I	Vnitřní	Vnitřní prostory, stálá teplota a vlhkost
Třída prostředí II	Vnitřní - všeobecné	Vnitřní prostory s teplotními rozdíly $-10^{\circ}\text{C}$ až $+40^{\circ}\text{C}$ (chodby, sklepy, garáže, možnost kondenzace vlhkosti na oknech)
Třída prostředí III	Venkovní – chráněné nebo extrémní vnitřní podmínky	Vně budov s teplotními rozdíly $-25^{\circ}\text{C}$ až $50^{\circ}\text{C}$ , mimo přímé povětrnostní vlivy
Třída prostředí IV	Venkovní - všeobecné	Vně budov s teplotními rozdíly $-25^{\circ}\text{C}$ až $50^{\circ}\text{C}$ , přímé povětrnostní vlivy

Zdroj: [25]

## 2.2 Poplachové systémy – Kombinované a integrované systémy

Návrh a zřizování kombinovaných a integrovaných systémů se řídí dle ČSN CLC/TS 50398. Dle této normy se stanovují všeobecné požadavky na systém, norma popisuje typické konfigurace kombinovaných systémů. Dále poskytuje základní podklady pro prvotní návrh systému, plánování instalace, instalaci až po předání do trvalého provozu včetně plánu údržby. V tomto dokumentu jsou specifikovány požadavky na bezpečnostní technologie, které mají být s ostatními systémy (nemusí být bezpečnostní) integrovány.

### 2.2.1 Typy konfigurací

Všeobecně jsou v normě popsány tři typy konfigurací integrovaných poplachových systémů.

- **Typ 1** – kombinace a integrace jednoúčelových poplachových i nepoplachových systémů. Jednotlivé systémy jsou připojeny doplňkovou trasou k společnému systému. Jednotlivé systémy musí splňovat svoje aplikační normy.
- **Typ 2A** – kombinace a integrace poplachových systémů i nepoplachových systémů využívající společné trasy, zařízení, vybavení. Porucha kterékoli části systému nesmí vyvolat kolizi zbývajících systémů. Každý jednoúčelový systém musí splňovat své prováděcí normy.

- **Typ 2B** – V této konfiguraci může být integrita kteréhokoli normou vyžadovaného poplachového zařízení v jakékoli aplikaci ovlivněna poruchou v jiné aplikaci.

### 2.2.2 Systémové požadavky

Integrovaný poplachový systém v běžném provozu, ve stavu klidu nebo stavu poplachu nesmí být ovlivněn, ani nesmí ovlivňovat žádnou jinou aplikaci. V rámci kombinovaných a integrovaných systémů se využívá povelových signálů, ty mohou být přenášeny mezi aplikacemi nebo z ústředního ovládacího zařízení do dalších aplikací. Aby nedocházelo k nežádoucím činnostem v rámci dálkové správy budov a areálů, je důležité určit během zpracování návrhu požadované povelové činnosti, případně určit úrovně povolených činností přístupovými úrovněmi. Signalizace informace může být poskytnuta na společném signalizačním a ovládacím zařízení a musí být jasná a jednoznačná. Informace musí být signalizovány v pořadí priorit podle poplachových signálů vztahujících se k ochraně života, k ochraně majetku a nedovoleného vniknutí a signálů z ostatních poplachových systémů. Dále podle poruchových signálů ze systémů k ochraně života a majetku, poruchových signálů z ostatních poplachových systémů a informací z nepoplachových systémů. Všeobecně platí, že kromě zobrazovaných informací musí být k dispozici doplňkové informace. Dále platí že, jednou zobrazený, ale stále se opakující signál nesmí být zobrazen, musí být zobrazeno že, existují signály z ostatních aplikací. A současně jakákoli činnost nesmí zamezit zobrazení aktuálního poplachu. Software pro společné vyhodnocovací prvky musí být oddělen od jednotlivých poplachových aplikací. Centrální ovládací zařízení je členěno do dvou tříd. **Třída 1** povoluje požit toto zařízení v prostoru, kde jsou instalovány ovládací prvky poplachových systémů. Zařízení ve **Třídě 2** musí odpovídat aplikačním normám poplachových systémů [26].

## **II. PRAKTICKÁ ČÁST**



### 3 ZABEZPEČENÍ BUDOVY U5

#### 3.1 Úvod

Budova U5, je jeden z objektů Univerzity Tomáše Bati ve Zlíně, je situována do katastrálního území Zlín, Jižní Svahy, Nad Čepkovem mezi ulice Nad Stráněmi a Družstevní. Jsou zde umístěny: Fakulta aplikované informatiky, Fakulta technologická, Fakulta managementu a ekonomiky, Ústav tělesné výchovy a Menza.

##### 3.1.1 Identifikační údaje stavby

Adresa objektu:

Univerzita Tomáše Bati, Fakulta aplikované informatiky

Nad Stráněmi 4511

760 05 Zlín, Jižní Svahy

Česká republika

##### 3.1.2 Podklady

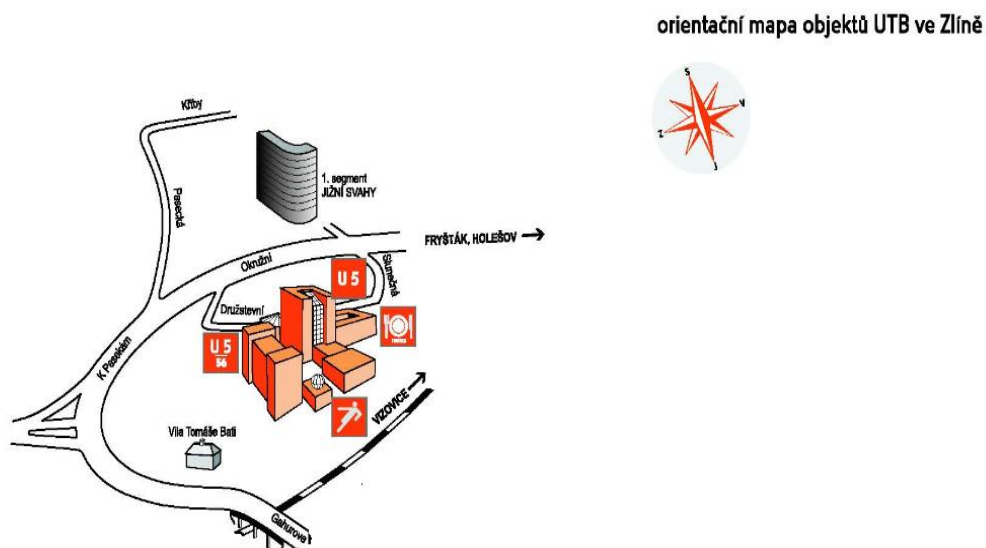
- Dokumentace stavebního řešení (SO)
- Konzultace se správou budovy
- Obhlídka objektu
- Platné ČSN

##### 3.1.3 Situace

Okolí budovy je volně přístupné pro veřejnost, objekt není oplocen ani nijak vymezen jeho perimetr. Plášť budovy je tvořen betonovým skeletem, výplně otvorů jsou tvořeny kovovými rámy oken a dveří s výplní ze skla. V bezprostřední blízkosti u přilehlé cesty na ulici Nad Stráněmi je parkoviště pro zaměstnance fakulty. Vjezd je ošetřen zákazovou dopravní značkou č.B1 - zákaz vjezdu všech vozidel s dodatkovými tabulkami s výjimkou pro vjezd vozidel IZS a zaměstnanců univerzity. Hlavní vstupní prostor je orientován na sever, pobytové prostory jsou orientovány částečně východním a převážně jihozápadním směrem. Ostatní vstupy do budovy jsou považovány za služební, zásobovací nebo technické. Koncepce budovy vychází z prostor vzájemně volně průchozích stavebních objektů SO51, SO52, SO53, SO54 SO55. V části SO51 se jedná se o osmipodlažní budovu převážně

s kancelářskými prostory, v části SO53 o budovu se 3 nadzemními podlažími s učebnami a laboratořemi, a v části SO52, SO54, SO55 o budovu do úrovně dvou nadzemních podlaží. Uspořádání prostor je řešeno tak, aby bylo zajištěno denní osvětlení pracovišť a zároveň omezena tepelná zátěž zaměstnanců slunečním zářením. Objekt je v částech SO51 vybaven dvěma osobními, a v SO53, 54 jedním osobním a jedním nákladním výtahem. Ve východní části budovy jsou situovány služební vchod, rampa a manipulační prostor pro zásobování budovy. Dále trafostanice, laboratoře pro zpracování polymerů a kotelna. Všechny tyto prostory mají samostatný vstup. Další samostatné vstupy jsou pro Ústav tělesné výchovy a to z východní a západní strany objektu. Na této straně je také spojovací koridor do Vědeckotechnického parku ICT v budově U5/56.

Obrázek 6 Situace U5



Zdroj: [27]

## 3.2 Základní technické údaje

### 3.2.1 Rozvodné soustavy

- |                    |                          |
|--------------------|--------------------------|
| • NN:              | 3PE N 400V/50Hz TN-C-s   |
| • Provozní         | 230V/50Hz TN-C-s         |
| • Slaboproudé PZTS | 12V <sub>ss</sub> , SELV |
| • Slaboproudé SKV  | 12V <sub>ss</sub> , SELV |
| • Slaboproudé CCTV | 230V/50Hz                |
|                    | 24V <sub>st</sub> , SELV |

### 3.2.2 Ochrana před úrazem elektrickým proudem

Základní ochrana před nebezpečným dotykovým napětím živých částí je provedena krytím a izolací, při poruše je provedena samočinným odpojením od zdroje v síti TN-C-s a malým napětím SELV/PELV.

### 3.2.3 Prostředí dle ČSN EN 50131-1

Vnější vlivy uvnitř budovy (vnitřní prostory) normální, prostor bezpečný.

Vnější vlivy venkovní prostředí AA7 (-25°C - +55°C), AB8 (-50°C - +40°C – vnější prostory nechráněné před sluncem a mrazem), prostor zvlášť nebezpečný.

## 3.3 Zhodnocení rizik

Budova se nachází v oblasti zastavěné bytovými domy v klidové zóně městské části Zlín - Jižní Svahy. Svojí volně dostupnou polohou pro procházející a vstupující osoby s úmyslem škodlivého působení je snadno dostupná, zranitelná. Ohrožení na lidských životech z hlediska jakéhokoli útoku se nepředpokládá, nelze jej však vyloučit. Předpoklad pokusu o poškození hmotného majetku, pokusu o poškození nebo krádež je však trvalý. Dle statistik PČR (Krajské ředitelství Zlín) došlo v období let 2010 – 2015 na území Zlínského kraje v průměru k 15-ti krádežím vloupáním do škol za rok.

Tabulka 4 Statistika krádeží vloupání do škol

Období	Počet	Škoda
1.1. - 31.12 2010	21	178000,-
1.1. - 31.12 2011	7	69000,-
1.1. - 31.12 2012	14	310000,-
1.1. - 31.12 2013	26	548000,-
1.1. - 31.12 2014	15	569000,-
1.1. - 31.12 2015	7	54000,-
1.1. - 31.3 2016	1	27000,-

Zdroj: [2]

Dalšími faktory, které navyšují hmotné škody, jsou vandalství, sprejerství.

### 3.4 Stávající elektronické zabezpečovací systémy

V současné době jsou v budově U5 instalovány systémy elektronických bezpečnostních technologií pro zabezpečení požadovaných částí objektu z hlediska ochrany majetku (PZTS), pro kontrolu vstupu osob z hlediska zamezení přístupu nežádoucích osob do vymezených prostor (SKV), pro monitorování pohybu osob v okolí budovy z hlediska prevence (CCTV). Dále je instalován systém elektrické požární signalizace pro včasnou detekci vznikajícího požáru (EPS), dorozumívací zařízení (DZ) pro komunikaci s ostrahou od vstupních dveří. Technickými parametry odpovídají době rekonstrukce objektu. Vzhledem ke svým vlastnostem byly považovány za nejlepší ve své kategorii.

#### 3.4.1 PZTS

Systém GALAXY 504.

Systém pro elektronické zabezpečení objektů dle ČSN EN 50131 do Stupně 3 v třídě prostředí II. Jedná se o modulární sběrníkový systém se čtyřmi komunikačními linkami RS485. K těmto linkám lze připojit kombinaci 16 vstupně/výstupních modulů RIO pro vyhodnocení až osmi detektorů, 7 ovládacích klávesnic MK 7 nebo 8 čtecích modulů např. MAX, MAXM200. Tyto kombinace platí pro všechny komunikační linky. K ústředně je připojen komunikační modul, který lze připojit pouze na první komunikační linku. Prostřednictvím tohoto modulu je zprostředkován přenos poplachové informace na DPPC bezpečnostní agentury. Výstup poplachové informace je také přenášen na ovládací klávesnice systému do prostoru stálé obsluhy na recepci 1.np. V systému může být zadáno 100 uživatelských kódů.

Obrázek 7 Ovládací panel PZTS GALAXY-MK7



Zdroj: [28]

Celý systém je rozdělen do jednotlivých grup (subsystémů) podle uživatelských potřeb. Subsystém nebo skupina subsystémů je přidělena jednotlivým uživatelům. Každá manipulace se systémem PZTS je ukládána do systémové paměti událostí. Podle dostupných informací, stávající systém není datově propojen s jinou bezpečnostní technologií např. SKV nebo CCTV.

### 3.4.2 SKV

Systém kontroly vstupu je řešen technologií od firmy Cominfo, a.s Zlín. Stávající systém je modulární, je tvořen řídicí jednotkou, čtečkami systému, dveřními jednotkami a elektromagnetickými otevírači, dále napájecími a záložními napájecími zdroji. Čtečky se snímací hlavou L-PRO-WIEGAND, které pracují s frekvencí 125kHz (LF), jsou rozmístěny u vybraných přístupových míst s potřebou omezit nebo zamezit volnému pohybu příchozích osob. Řídicí jednotky jsou použity REI:MP a REA:MP s vlastním nebo sdíleným napájecím zdrojem. Každá řídicí jednotka umožňuje obsloužit až čtyři snímače. Komunikace řídicích jednotek je prostřednictvím ethernetu. Jsou datově připojeny k centrálnímu serveru, na kterém také běží služby CARDPAY, PASSPORT, ACCESS a čerpají ze společné databáze. Uživatelé jsou vybaveni identifikační kartou EM Microelectronics H4102, (125kHz, 26bit) s identifikačním číslem držitele, platností karty a označením zda se jedná o zaměstnance nebo studenta. Karty pro návštěvy nebo servisní pracovníky jsou uloženy na recepci objektu.

Obrázek 8 Snímací prvek Comifo L-PRO, L-PRO/K



Zdroj: [29]

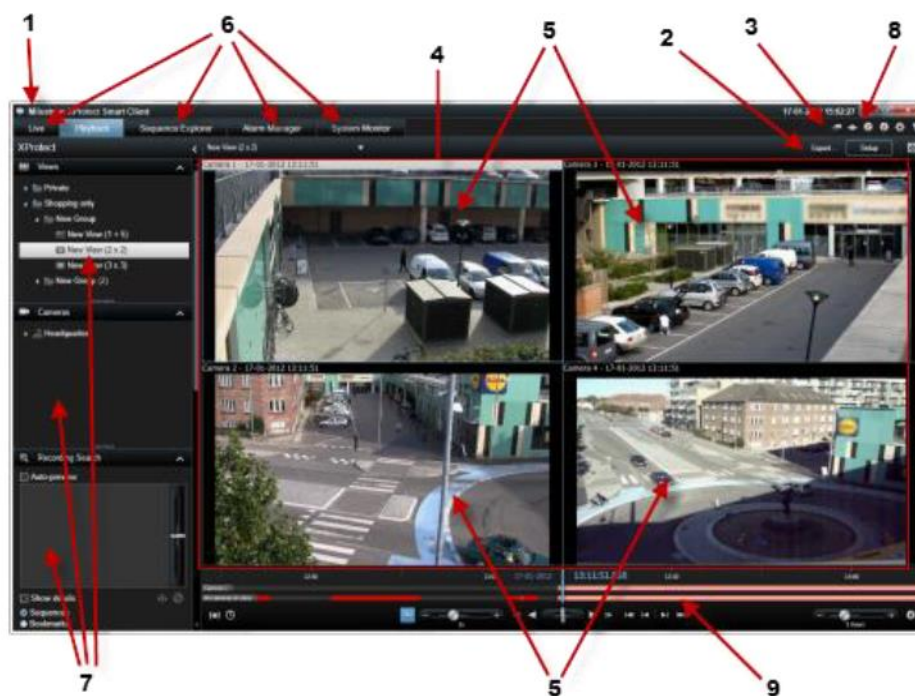
Identifikační karty prostřednictvím indukovaného napětí z antény vysílají svoje identifikační číslo, které je porovnáno s uloženými daty a následně umožněn přístup. Elektromagnetické otvírače pracují v reverzním módu, tzn., že při odpojení napájecího napětí jsou uvolněny a je možný bezpečný odchod z místnosti, budovy. Systém kontroly vstupu je prostřednictvím NC výstupů napojen k systému EPS

### 3.4.3 CCTV

V objektu U5 je instalován systém CCTV pro monitorování a záznam běžného provozu budovy. Systém je tvořen přehledovými kamerami v provedení do vnitřního prostředí a dále v krytu do venkovního prostředí. Ve vztahu k průchodu osob se jedná o monitorovací prostředek se záznamem aktivity v zájmové oblasti. Výstupní signál je vyveden do prostoru recepce na úrovni 1. nadzemního patra. Napájení kamer je 230V/50Hz, přisvětlení venkovních kamer je řešeno díky veřejnému osvětlení (někdy nedostatečné), přisvětlení vnitřních kamer je také prostřednictvím zbytkového světla z veřejného osvětlení. Jedná se o kombinaci analogových a IP kamer, které jsou ukončené enkodérem a převedené do úložiště NVR. Systém pracuje v tzv. triplexním režimu, kdy je schopen v jednom okamžiku zaznamenávat obraz, zobrazovat scény i z ostatních kamer v reálném čase, případně vyhledat a přehrávat záznam. V recepci na monitorovacím a klientském pracovišti je instalován SW klient Milestone XPROTEC Smart v2.14. Jedná se o volně dostupnou aplikaci pro práci s obrazem živým i ze záznamu. Aplikace umožňuje monitorovat externí vstupy systému, např. alarm z PZTS budovy. Aplikace upozorňuje např. na vznik aktivity v zájmové oblasti monitorované systémovou kamerou. Díky řešení prostřednictvím systémů NVR

a klientských pracovišť je možné monitorovat celý prostor z centrálního monitorovacího pracoviště a k vzniklé události bezprostředně vyslat zásahovou jednotku.

Obrázek 9 CCTV Klientské pracoviště



*Legenda:*

1. Záhlaví aplikace, 2. Panel nabídek pracovního prostoru, 3. Panel nástrojů, 4. Okno aktivního náhledu, 5. Okno náhledu, 6. Záložky aplikací, 7. Panely připojených zařízení, 8. Panel aplikací, 9. Časová osa

Zdroj: [30]

Rozmístění jednotlivých kamer v objektu.

- Hlavní vstup - příchodová
- Ústav tělovýchovy a sportu vstup - příchodová
- Zadní vstup vnitřní - příchodová
- Rampa a manipulační prostor - přehledová
- Parkoviště služební - přehledová
- Hřiště - přehledová (IP)
- Tělocvična - přehledová
- Posilovna - přehledová
- Kopírka, Vstup U56 - zájmová

Ke spolehlivému provozu systému CCTV je nezbytné zajistit alespoň minimální osvětlení i v nočním režimu.

#### 3.4.4 DZ

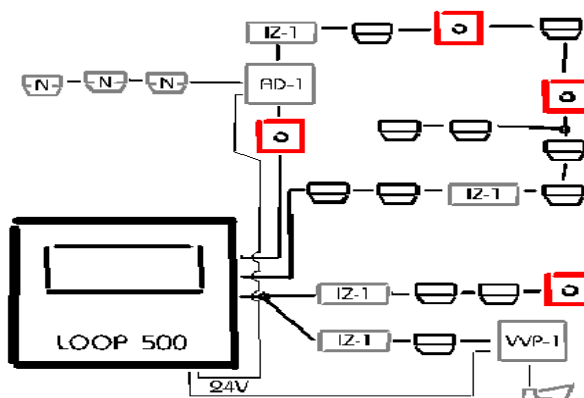
Dorozumívací zařízení v objektu U5 je řešeno prostřednictvím analogového systému dveřních komunikátorů. Komunikační panely v provedení do venkovního prostředí, jsou umístěny u vybraných vstupů, ovládací tlačítka volby hovoru jsou nasměrována prostřednictvím analogového přepínače na ostrahu v recepci objektu. Ostraha po autorizaci vstupující osoby, může prostřednictvím svého telefonu ještě v hovoru odblokovat dveřní otevírače.

#### 3.4.5 EPS

Zařízení elektrické požární signalizace je soubor technických prvků a zařízení dle ČSN 34 2710, ČSN EN 54-2,4 sloužící k včasnému zjištění začínajícího požáru. Systém EPS nemůže zamezit vzniku požáru. Jeho instalace má především preventivní charakter. Ve vztahu k průchodu osob systém EPS umožňuje volný odchod z budovy, a to aktivací výstupů ovládající napájení elektromagnetických nebo elektromechanických otvíračů systému SKV. Je tak usnadněna evakuace osob v případě vzniklého požáru. V budově U5 jsou instalovány systémy: EPS LOOP 500 od firmy TYCO – Zettler a EPS IQ8 M od firmy ESSER GmbH. Jedná se o adresovatelné systémy elektrické požární signalizace. Systém EPS se skládá z několika funkčně propojených částí, kterými jsou hlásiče, vstupní výstupní moduly pro připojení vyhrazených požárně bezpečnostních zařízení (požární klapky, požární ventilátory pro odtah tepla a kouře, uvolnění dveří na chráněných únikových cestách, akustická signalizace atd.). Základní sestava ústředny obsahuje zdrojovou část, základní vyhodnocovací desku s monitorovanými reléovými výstupy pro sirény a volnými porty pro možnost rozšíření systému a zobrazovací a ovládací jednotku. Základní desky ústředny jsou vybaveny porty pro připojení (v případě LOOP 500 čtyř liniových vedení požárních hlásičů tj. 1 – 63 hlásičů k jedné lince). Pomocí desky DV1 je systém rozšířen o další hlásičové linky. Celkový počet liniových vedení je 8, prostřednictvím hardwarového propojení jsou zapojeny na čtyři kruhové linky pro max. 126 hlásičů na každé kruhové lince.



Obrázek 10 EPS LOOP 500 Kruhové vedení



Zdroj: [31]

V případě ústředny IQ8 M lze po rozšíření systému třemi linkovými kartami připojit čtyři kruhová vedení. Základní sestavy ústředny lze doplnit deskou reléových výstupů nebo deskou signalizace stavů skupin hlásičů. Požární hlásiče jsou rozmístěny na určených místech a v určených prostorách a svými vlastnostmi a charakteristikou odpovídají danému prostředí (rychle hořící látky, látky uvolňující při hoření agresivní nebo jedovaté chemikálie, látky, které uvolňují velké množství kouře apod.) Hlásiče identifikují poplachové podněty a informace která vzniká na výstupu jednotlivých hlásičů, je pak předána kruhovým vedením do ústředny EPS. Ty zajistí zpracování a následnou aktivaci výstupních obvodů. Celý systém je programově rozdělen do skupin hlásičů, které odpovídají požárně bezpečnostnímu řešení stavby zpracovanému dle vyhlášky 246/2001 Sb. o stanovení podmínek požární bezpečnosti a výkonu požárního dozoru. ČSN 730875 Požární bezpečnost staveb – Stanovení podmínek pro navrhování EPS v rámci požárně bezpečnostního řešení, ČSN 730802 Požární bezpečnost staveb – Nevýrobní objekty. Výstup poplachové informace je signalizován akustickou signalizací, rozmístěnou v objektu a na ovládacím panelu systému EPS v prostoru recepcie v 1. nadzemním patře. Systém EPS je připraven pracovat v režimu DEN, kdy je při vyhlášení poplachu spuštěn čas T1. V tomto intervalu je ostraha objektu povinna potvrdit na ústředně stanoveným postupem přijetí poplachové informace a zajistit kontrolu místa vzniku požáru. Na kontrolu místa spuštěn časový interval T2. Po ukončení tohoto intervalu jsou samočinně aktivovány výstupy systému EPS. V režimu NOC, tzn. bez obsluhy, jsou všechny naprogramované výstupy spouštěny okamžitě, stejně jako v případě aktivace manuálních hlásičů v kterémkoli z režimů.

### 3.4.6 MZP

Mechanické zábranné prostředky jsou považovány za základní prvek technické bezpečnosti, jako první znesnadňují nebo přímo zamezují vniknutí do zájmového prostoru, objektu. Objekt U5 je z hlediska mechanických zábranných prostředků vybaven standartními otvory výplněmi a uzamykacími systémy BT 2, nebo BT 3 dle EN 1627 a EN 1303. Klíčové hospodářství je řešeno systémem generálního klíče pro technické a technologické místnosti, na ostatní pobytové a kancelářské prostory se systém generálního klíče nevztahuje. Z hlediska omezení volného průchodu osob v okolí budovy je zřejmá absence oplocení v celém obvodu pozemku. Lze předpokládat, že oplocení není instalováno z důvodu uvedeného ve vyhlášce 268/2009 Sb. o požadavcích na stavby §7 kdy oplocení nesmí svým rozsahem tvarem a použitým materiálem narušit charakter stavby a jejího okolí.

### 3.4.7 Fyzická ostraha, režimová opatření

Fyzická ochrana budovy U5 je realizována zaměstnancem soukromé bezpečnostní služby na základě pověření uvedeného v obchodní smlouvě. Zaměstnanec vykonává činnost na stálém stanovišti v uzavřené recepci, která se nachází na úrovni 1n.p.. Služba je z časového hlediska celodenní a je rozdělena na dvě dvanáctihodinové směny pro jednoho zaměstnance. V průběhu denní služby plní pracovník SBS funkci recepčního, provádí telefonická spojení, provádí výdej klíčů a přístupových karet dle pověření, podává informace o přítomnosti zaměstnanců univerzity. Vykonává dohled nad elektronickými zabezpečovacími systémy. V případě poplachové události na kterémkoli bezpečnostním systému je odesílána zpráva správci objektu. Ve společné součinnosti s pracovníkem SBS jsou podniknuta potřebná opatření. V průběhu noční služby jsou po odchodu zaměstnanců univerzity zastřeženy všechny části objektu a zaměstnanec SBS monitoruje bezpečnostní technologie a v případě události informuje centrální dohledové pracoviště. Noční kontrola neporušenosti pláště budovy je prováděna motorizovanou hlídkou vyslanou z operačního střediska. Délka a pravidelnost prováděných kontrol je dle potřeby, dostupných informací a podle rozhodnutí operačního střediska Odblokování střežených prostor proběhne pracovníkem SBS s příchodem prvního zaměstnance fakulty.

## 3.5 Zhodnocení

Elektronické bezpečnostní systémy instalované v budově U5 jsou plně funkční, svými naprogramovanými aktivitami v rozsahu svých technických možností plně podporují ochranu

osob a majetku, monitorování průchodu osob nebo jejich záznam o pohybu. Technické řešení instalovaných systémů odpovídá době rekonstrukce objektu. Instalované technologie, jejich provedení a provedení realizace odpovídá platným legislativním předpisům. Koncepce bezpečnostních technologií je však rozdělena do mnoha ovládacích prvků a prvků pro jejich správu. Pro každou technologii je nutnost zadávat a přidělovat oprávnění uživatelům odděleně. V případě požadavku na rozšíření systému PZTS může dojít k naplnění kapacity systému, podobně jako v případě požadavku na nový doplněk v SW vybavení ústředny, např. online správu systému bez jeho odstavení z provozu. Celkové technické řešení zabezpečení poskytuje v některých částech, zejména na perimetru a plášti budovy, možnost přístupu a následného pokusu o vniknutí do objektu bez možnosti těmto pokusům předejít (absence CCTV a samostatného přisvětlení snímané scény). V případě poplachové události se ostraha spoléhá na ostatní bezpečnostní systémy. Vzhledem technickým možnostem systémů se obsluha získává informace z displejů systémových ovládacích panelů (většinou 2x16 znaků). Dá se předpokládat náročnost ovládání z hlediska nedostatečných informací a s tím spojená nepřehlednost systému. Následkem je reakce ostrahy s dlouhou dobou odezvy.

Elektronické monitorování a záznam průchodů osob do budovy v denním režimu není možný. U hlavních vstupů nejsou k dispozici žádné identifikační ani počítačící zařízení. Ostraha nemá možnost určit přesný počet osob v budově, např. pro případ nutnosti jejich evakuace. Ostraha nemá možnost získat informaci o tom, zda v průběhu denního režimu nedochází k bezpečnostním incidentům ve studovnách nebo na chodbách. Používaná technologie identifikačních karet „EM Microelectronics H4102, 125kHz“ je v současnosti na ústupu. Pro snadnou dostupnost SW prostředků pro čtení informací na přenosném médiu a možnosti následného kopírování.

Bezpečnostní riziko a ohrožení areálu, objektu ve vztahu k průjezdu vozidel, může nastat také v případě neoprávněného parkování nepovolených vozidel na vyhrazeném parkovišti univerzity v bezprostřední blízkosti budovy nebo na služebním parkovišti před manipulačním prostorem.

Množství bezpečnostních systémů, které pomáhají chránit budovu, činnost ostrahy v případě vyhodnocení poplachové situace pro svoji nepřehlednost komplikuje.

## 4 NÁVRH DOPLNĚNÍ ZABEZPEČENÍ

### 4.1 Úvod

Tato část práce navazuje na předchozí kapitoly návrhem na doplněním stávajících bezpečnostních technologií. Vzhledem k předpokládané etapizaci realizace z hlediska časové náročnosti a finančního rozvržení, jsou návrhy technických řešení rozděleny podle jednotlivých technologií. Je možná i vzájemná kombinace.

- Návrh doplnění SKV
- Návrh doplnění PZTS
- Návrh doplnění CCTV
- Návrh úpravy MZP
- Návrh integrace systémů, grafická nástavba
- Návrh nové technologie PZTS, SKV

Rozdělení dle technologií bude ctít také ekonomická rozvah<sup>o</sup>; je součástí této práce.

### 4.2 Doplnění stávající technologie

#### 4.2.1 Doplnění SKV

V návrhu doplnění se zabývám možnostmi doplnit bezpečnostní technologie pro kontrolu a monitorování vstupu s využitím stávajících technologií systému SKV.

V této práci, v části zhodnocení jsem uvedl, že ostraha objektu nemá žádnou možnost kontroly nebo získání informace o počtu osob, které se právě nacházejí v budově. Tyto informace mají důležitý charakter v případě poplachové situace a nutnosti evakuace osob. Dále nemůže(ani na dálku) zamezit vstupu nebo úniku podezřelých osob. Z důvodu zajištění vyšší bezpečnosti studentů a zaměstnanců, v souladu s pokyny ke stanovení úrovně zabezpečení škol dle AGA, navrhuji doplnit ke všem samostatným vstupům příchodové a odchodové čtečky s elektromechanickými samozamykacími zámky a dveřními samozavírači. Před hlavní vstup a výstup přisadit rotační turnikety a elektromechanické zábrany s blokovanou brankou pro návštěvy a servisní pracovníky. Provedení turniketu a zábran do venkovního prostředí bude s odpovídající povrchovou úpravou a bude korespondovat s prosklenou fasádou objektu. Dále v prostoru zádveří hlavního vstupu provést rozdělení

na dva samostatné průchody a doplnit je vstupně / výstupními kamerami s nainstalovaným SW (tzv. people counter) jako doplněk SKV pro další kontrolu počtu vstupujících osob.

#### **4.2.1.1 Doplnění snímacích zařízení k samostatným vstupům.**

Snímací zařízení pro kontrolu vstupu budou doplněna v SO 512, SO 513. Jedná se o prostory z východní strany objektu u manipulačního prostoru a nakládací rampy.

- C116 – C118 Zádveří
- C112 Rampa – C118 Zádveří
- C112 Rampa – C107 CNC technologie
- C112 Rampa – C111 Trafostanice
- Vstup – C108 Zpracování polymerů
- Vstup – C109
- Vstup – C110

Snímací zařízení budou připojena do čtyř řídicích jednotek umístěných v chodbě C104 a místnosti C108. Datové rozvody budou provedeny kabely SFTP min. cat.5e, zakončeny konektory RJ 45 a připojeny do řídicích jednotek. Napájecí rozvody budou provedeny kabely H05VV-F 4x1mm<sup>2</sup>. Kabely budou uloženy v ohebných trubkách v podhledech nebo vloženy v PVC lištách přisazených na omítku. Řídicí jednotky budou připojeny prostřednictvím průmyslových switchů na samostatná optická vlákna nové optické sítě. Optická síť bude průběžná, vedena chodbami 1.np v ohebných trubkách v podhledu na samostatných příchytkách a rozvody budou řádně označeny: „POZOR OPTICKÝ KABEL“. Optická kabeláž bude v provedení vícevidového kabelu MM 50/125, OM2 kdy je zaručen přenos gigabitového ethernetu na vzdálenost 550m. Hlavní optická síť bude využita také pro systém CCTV. V blízkosti umístění koncového prvku, řídicí jednotky, bude optická kabeláž ukončena v nástěnné skříni s výbavou pro ukončení optických vláken a prostorem pro umístění průmyslového switchu. Ke každé skříni bude přivedeno napájecí napětí 230V/50Hz ze samostatně jištěného přívodu pro napájení průmyslových switchů.

#### **4.2.1.2 Doplnění turniketů**

Další opatření pro zamezení vstupu nežádoucích osob do objektu je opatření u hlavního vstupu do budovy. Vybudováním dvou jednosměrných rotačních turniketů s funkcí antipanik (sklopná ramena), snímacími a signalizačními prvky u obou vstupních dveří. Propustnost turniketu je 30 osob za minutu. Pomocí tohoto řešení bude zajištěna regulace osob při

vstupu, výstupu a jistý přehled o počtu osob v budově U5. Ostraha bude mít možnost zamezit vstupu, případně úniku nežádoucích osob do a z budovy blokovacími tlačítky v prostoru recepce. Provedení turniketu a směrových zábran bude korespondovat s prosklenou stěnou vstupního portálu budovy U5. Směrové zábrany budou s přídržnými elektromagnety v patě konstrukce (brance). Bude tak zajištěno uvolnění zábran od EPS v případě požáru a uvolnění únikových cest. Návrh vstupního turniketu bude ve spolupráci s výrobcem např. Cominfo a.s. Zlín. Doplnění SKV bude systémové, snímací jednotky budou připojeny kabely SFTP min. cat.5e do řídicích jednotek systému SKV. Řídící jednotka, která bude obsluhovat snímací prvky v turniketu, bude umístěna v recepci a propojena do celkového systému SKV. Na recepci bude instalovaný klientský SW pro možnost zobrazení identifikačních údajů procházejících osob a všech dostupných stavů systému (nepovolené otevření dveří, překročení limitu otevřených dveří atp.). Všechny řídicí jednotky čerpají uživatelské role z databáze uložené na centrálním serveru. Vzhledem k tomu, že komunikace řídicích jednotek probíhá po ethernetu, lze celý systém rozšiřovat podle potřeb zadavatele. Je omezen jen rozsahem poskytnutých IP adres.

#### **4.2.1.3 Ovládání**

Vzhledem k tomu, že se jedná o návrh rozšíření stávajících technologií, zůstávají požadavky na obsluhu, zadání, výdej a evidenci identifikačních karet v nezměněné podobě.

#### **4.2.1.4 CCTV People Counter**

Jako další prvek pro podporu ověření počtu osob v objektu navrhuji instalovat před zádveří u výstupu kameru s instalovaným SW (people counter), např. AXIS 209FD SW True View People counter.

Obrázek 11 People counter



Zdroj: [32]

Kamera bude umístěna na středu průchodu tak, aby monitorovala kolmým pohledem zájmový prostor. Kamera bude připojena prostřednictvím ethernetu do datové sítě, napájení bude ze zálohovaného zdroje 12V-DC/4A, umístěného v technické části recepcce. Výstupní signál bude zobrazen na recepci jako jedna z aplikací na klientském PC SKV. V nastavení této kamery bude provedena kalibrace prostoru a jeho rozdělení na zóny pro vstup a výstup do objektu. Snahou tohoto řešení je upřesnit počet osob při pokusu o průchod více osob dveřmi, turniketem na jednu identifikační kartu.

#### **4.2.1.5 Návrhy prvků**

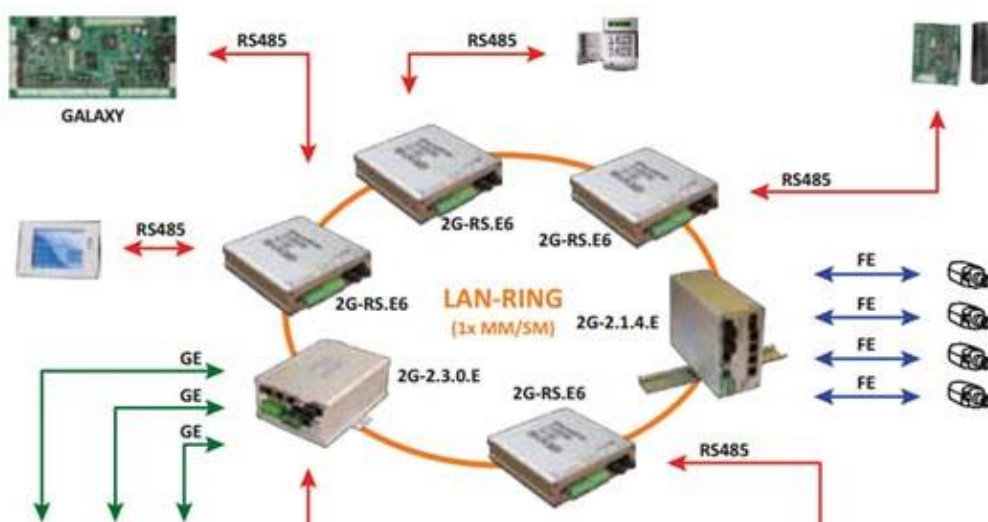
Navrhované prvky v případě rozšíření SKV budou vzhledem k nutnosti kompatibility stejné, jako je uvedeno v části „zhodnocení“. V případě doplnění CCTV PC pro SKV např. AXIS 209FD SW True View People counter. Navrhovaný průmyslový switch např. 2G-2s.0.3.FC-BOX LAN RING, navrhované skříně pro optickou síť např. Univers Z 550/800/250.

#### **4.2.2 Doplnění PZTS**

Doplnění stávajícího systému PZTS vychází z důvodů uvedených v úvodu práce. Kdy v případě vstupu nežádoucí osoby a vzniku nutnosti přivolání pomoci bude možno tento krok provést. Návrhem je doplnění nouzových (tísňových) tlačítek alespoň do chodeb v prostoru učeben, laboratoří, k schodištím, únikovým východům a nejlépe také přímo do jednotlivých přednáškových sálů. Výstup poplachové informace zůstane v prostoru recep-

ce. Pracovník SBS tento nouzový požadavek může řešit okamžitě. Je to jeden z prvků, kdy bude splněn požadavek metodického doporučení o minimálním standardu bezpečnosti studentů v budovách školy. Předpoklad je připojení nových tísňových smyček k volným vstupům stávajících linkových modulů systému PZTS a v případě nutnosti doplnění také linkových modulů. S výhodou je možno využít zónového zapojení smyček např. v chodbě B201 pro více tlačítek. Další způsob, jak zdokonalit stávající systém PZTS a využít jeho možností nejen k ochraně před narušiteli, je doplnění nouzových tlačítek s táhly do prostoru WC pro imobilní. Stejně jako v předchozím případě bude ostraha o vzniklé nouzi informována okamžitě. Programové nastavení nouzových smyček bude jako 13=PA, jeho funkce tak bude nepřetržitá. Pro kontrolu vykonaného zásahu bude možnost rušení poplachu omezena pouze po aktivaci nově instalovaných klíčových spínačů v blízkosti těchto tlačítek. Jedná se o prvek, který je v souladu s požadavky vyhlášky č.398/2009 o bezbariérovém užívání stavby, kde je podrobně popsáno umístění těchto prvků. Kabeláž k novým prvkům bude provedena ve stávajících rozvodech slaboproudých instalací. Nutnost doplnění pomocných napájecích zdrojů se záložním akumulátorem bude pouze v případě nutnosti doplnit linkové moduly případně pro další ústředny PZTS.

Obrázek 12 Topologie LAN RING



Zdroj: [33]



#### 4.2.2.1 Návrhy prvků

Typy navrhovaných tlačítek pro stav nouze v učebnách a chodbách je např. ART 476, do prostoru WC pro imobilní pak např. FAP3002. Klíčový spínač pro resetování stavu nouze např. typ NICE.

#### 4.2.3 Doplnění CCTV

Vzhledem nedostatečnému pokrytí perimetru monitorovacími prvky systému CCTV a absenci vlastního přisvětlení bude v návrhu doplnění těchto prvků. Doplněním kamer bude ostraze objektu zajištěna možnost monitorovat celkové okolí. Ostraha bude mít možnost v předstihu zamezit vstup podezřelým osobám a zabránit vzniku škod. Kamery uvedené v kapitole 3.5. doplnit automatickým přisvětlením s autonomním spínáním při setmění. Přisvětlení v provedení do venkovního prostředí doplnit ke každé kameře do stejného směru. Napájení a automatické spínání přisvětlení bude realizováno připojením k stávajícímu napájení kamer.

Doplnění prvků CCTV kamer včetně automatického přisvětlení v provedení IP do perimetru:

- Severní strana pláště budovy 2.np - směr okna 2.np - hlavní vstup
- Severní strana pláště budovy 1.np - směr hlavní vstup - okna chodba 1.np
- Severní strana parkoviště zaměstnanců
- Východní strana – směr trafostanice
- Východní strana – směr Manipulační prostor – laboratoře zpracování polymerů
- Jižní strana pláště budovy – směr služební vchod – okna 1.np
- Jižní strana vstup tělocvična zadní vstup
- Západní strana – směr tělocvična – hlavní vstup

Obrázek 13 CCTV Kamera s IR Přísvitem (kompakt)



Zdroj: [34]

Vzhledem k vzdálenostem a nově navrhované technologii IP CCTV navrhuji výstupní signál z kamer připojit prostřednictvím průmyslových switchů na samostatná optická vlákna nové optické sítě. Optická síť bude průběžná, vedena chodbami 1.np v ohebných trubkách v podhledu na samostatných přichytkách a rozvody budou řádně označeny: „POZOR OPTICKÝ KABEL“. Optická kabeláž bude v provedení vícevidového kabelu MM 50/125, OM2 kdy je zaručen přenos gigabitového ethernetu na vzdálenost 550m. V blízkosti umístění koncového prvku, kamery, bude optická kabeláž ukončena v nástěnné skříni s výbavou pro ukončení optických vláken a prostorem pro umístění průmyslového switche. Ke každé skříni bude přivedeno napájecí napětí 230V/50Hz ze samostatně jištěného přívodu pro napájení průmyslových switchů. Odtud bude kabeláž provedena datovým metalickým kabelem SFTP min.cat.5e ke každé z kamer, bude ukončen konektory RJ45. Napájení nových kamer včetně přísvitu bude v provedení PoE z průmyslového switche. Kamery budou v provedení kompakt do venkovního prostředí s automatickým přísvitem a možností ovládat jej centrálně. Pro podporu doplněného systému PZTS s nouzovými tlačítky, pro přivolání pomoci při napadení nežádoucí osobou, je nutné doplnit také systém CCTV o vnitřní přehledové kamery. Budou monitorovat průchozí chodby objektu do úrovně 3.np v objektu SO540, SO 532, SO 531 a SO513. Jedná se celkově o 19ks kamer rozmístěných v prostoru chodeb C303, C301, D301, D310, B201, C203, C201, D201, D210, A217, B110, C104a, C104, D101, D111, A116, A102.

Vyhodnocení signálu bude v prostoru recepcce na stávajícím klientském pracovišti a SW vybavení s možností upgradu na verzi X Protect Enterprise a vyšší, s možností vazby na přístupový systém. Serverové záznamové zařízení bude hybridní pro 32 analogových a 16

IP kamer s min 16TB HDD RAID 5. Není nutná okamžitá výměna všech stávajících kamer v systému. Pro nové IP kamery pak další server s podporou připojení až 40 IP kamer.

#### 4.2.3.1 Návrhy prvků

Navrhovaný typ kamer kompakt např. Sony SNC-EB632R 3 MPx, navrhovaný typ vnitřních kamer např. Sony SNC-VM631 polodome 3 MPx, navrhovaný typ záznamu pro rozšíření systému CCTV Milestone Husky M50, navrhovaný typ přisvětlení např. IRH60L8A (60°/40m), navrhovaný typ průmyslového switche je stejný jako pro systém SKV, Software pro vyhodnocení X Protect Enterprise.

#### 4.2.4 Provoz kamerového systému

Provozování kamerových systémů musí být v souladu se zákonem č.101/2006 Sb. o ochraně osobních údajů. Podle tohoto zákona se za zpracování osobních údajů považuje kromě sledování také pořizování záznamu získaných záběrů. Z hlediska tohoto zákona vyplývá pro správce kamerového systému oznamovací / registrační povinnost. Kamerový systém se záznamem lze provozovat v případech:

- Pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce
- Jestliže je zpracování nezbytné pro dodržení právní povinnosti správce
- Na základě souhlasu subjektů údajů

Udělení souhlasu se přitom týká pouze subjektů, které se v monitorovaném objektu vyskytují pravidelně (studenti, zaměstnanci). Zároveň je povinnost na viditelném místě označit monitorované prostory informační tabulkou („**objekt je monitorován kamerovým systémem se záznamem**“).

V případech provozování kamerového systému pro osobní potřebu (monitorování pouze soukromého pozemku, bytu, sklepa, parkovacího místa) nebo v případě provozování systému ze zvláštních povinností (např. zákon č.412/2005 Sb. OUI, zákon č.273/2008 Sb. o Policii ČR, zákon č.555/1992 Sb. o Vězeňské službě a Justiční stráží atp.) oznamovací / registrační povinnost odpadá [35].

#### 4.2.5 Úprava MZP

MZP uvedené v části 3.3.6 odpovídají použitým typem a provedením tříd prostředí i stupni zabezpečení. Při rozšíření systému SKV na turniketech je nutné dodržet prvky pro stejné třídy prostředí a stupně zabezpečení.

Z hlediska podpory rychlého zásahu navrhuji v prostoru recepcce demontovat část, případně celé prosklení, které zamezuje šíření zvuku a omezuje ta možnosti důrazného pokynu směrem k přicházející/unikající osobě. Dále pro podporu jistoty zásahu vytvořit průchod pro zásah/únik z recepcce přímo do hlavní vstupní haly objektu. Jedná se o demontáž a stavební úpravy části čelní stěny recepcce.

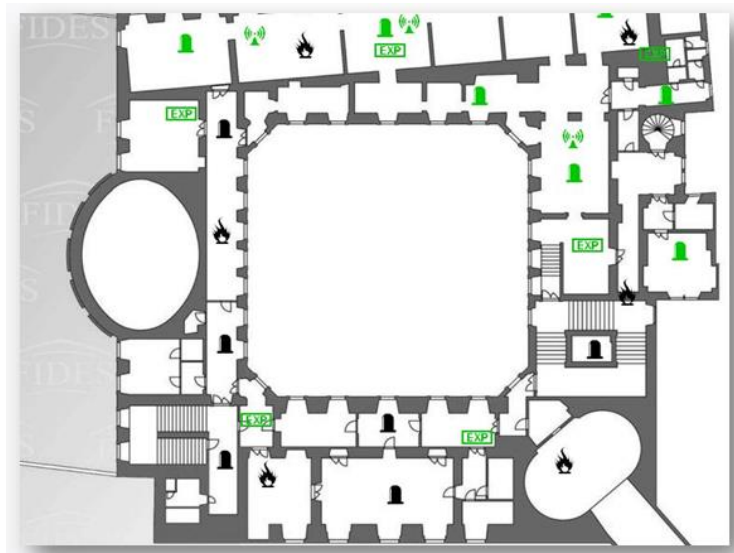
#### **4.2.6 Integrovaný, monitorovací a řídicí systém, grafická nástavba PZTS, SKV, EPS**

Pro zjednodušení a zpřehlednění obsluhy všech stávajících bezpečnostních technologií v budově U5, je v návrhu integrační, monitorovací a řídicí systém. Pro integraci jsem zvolil produkt LATIS SQL českého výrobce a dodavatele firmy TRADE Fides a.s. Tento systém je určen pro všechny aplikace dle rozsahu. Množství a velikost připojených objektů je téměř neomezená, lze vytvářet rozsáhlé areály, které obsahují několik těchto nástaveb.

Jednotlivé technologie mohou být připojeny do systému pomocí různých rozhraní (RS485, RS 232, LAN, GPRS, SMS, Morse Radio). V tomto řešení je navržena komunikace prostřednictvím TCP/IP. Data z technologií budou prostřednictvím LAN přiváděna na komunikační interface (software) systému, ten je zpracuje a zapíše do databáze. Komunikační interface umožňuje obousměrnou komunikaci pro zapisování a pro ovládání ze strany operátora. Operátor tak má možnost odesílat povely do jednotlivých technologií je tak možnost např. zastřežení / odstřežení, odvolání poplachu, aktivace výstupu provádět na dálku. Vybraná zařízení je možné na dálku aktualizovat odesláním firmware. Pro systém PZTS je nutné doplnit do systému komunikační modul „Galaxy Smart“ ve kterém již komunikační interface s LATIS SQL je instalován. Modul se připojuje k první komunikační lince. Pro ústředny EPS pak moduly pro převedení komunikace na TCP/IP a SW interface LESI a LZTI. Pro stávající systém SKV bude nutné komunikační rozhraní vytvořit. Díky integraci systému CCTV do LATIS SQL a jeho oboustranné komunikaci je pak ostraze objektu automaticky nabídnuta okamžitá vizuální kontrola prostoru vzniku poplachové události. Tento integrační systém lze využít jako DPPC pro monitorování a ovládání vzdálených objektů nebo jako lokální grafická nástavba, případně jako kombinace uvedeného. V tomto řešení bude využit jako lokální grafická nástavba. Propojením jednotlivých technologií prostřednictvím komunikačních kanálů tak uživatel získá správu všech systémů z jednoho pracoviště v jednotné a srozumitelné podobě. Pro správu všech připojených zařízení je nástroj správy systému LAT. Pro přesnou lokalizaci vzniku události je systém navázán na vlastní mapové podklady s využitím reálných GPS souřadnic včetně rozlišení podlaží. Gra-

fické zobrazení zájmových oblastí včetně konverze mapových podkladů z geobáze, vkládání grafických symbolů detektorů lze vytvořit a dále modifikovat prostřednictvím grafického nástroje LGLE. Operátor má k dispozici přehledné grafické zobrazení LOW.

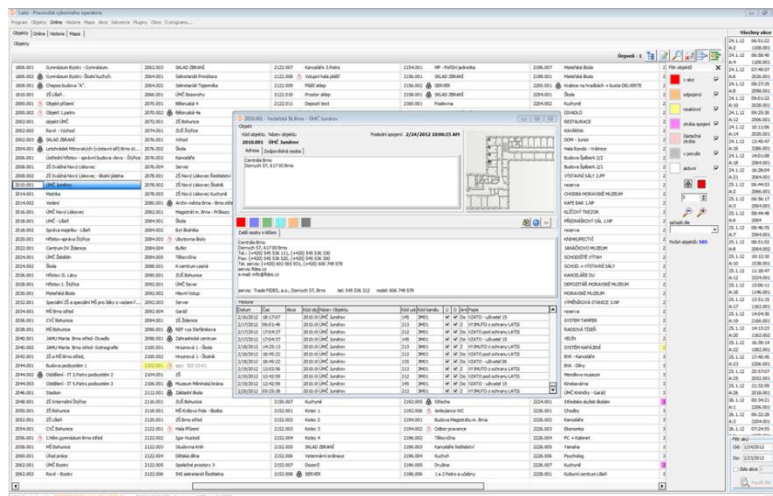
Obrázek 14 Grafické znázornění integrace PZTS, EPS



Zdroj: [36]

Zde je přehledně zpracován formou grafického zobrazení aktuální stav sledovaných prvků. Pro každý stav rozdílnou barvou a předem nastavenou akustickou signalizací. Dále je zobrazen textový výpis událostí. V případě vzniku mimořádné události jsou k dispozici automatická informační okna s příslušnými instrukcemi, které musí operátor provádět, nebo informační okna s kompletní dokumentací objektu. V tomto komunikačním prostředí může také operátor navázat spojení s nadřazeným, případně s jiným operátorem. Všechny události, včetně činnosti operátora (jakým způsobem řešil příšlou událost), jsou ukládány do historie systému. Historii systému lze jednoduše filtrovat. V rámci systému lze také nastavit vlastní přístupová práva pro různé úrovně přístupu.

Obrázek 15 Pracoviště operátora LOW



Zdroj: [36]

S přehledným a rychlým nástrojem lze také předpokládat efektivní odezvu ostrahy v případě poplachové události. Činnost operátora je s tímto nástrojem efektivní.

#### 4.2.6.1 Návrh prvků

PC klientská stanice – konfigurace

CPU Intel® Core i7-5775C (3.3GHz, 6M, LGA1150, VGA), ASUS Z97-P, 8GB DDR3-1600MHz Kingston HyperX Fury Blue, 2x4GB, HP NVIDIA Graphics PLUS NVS 315 1GB PCIe x16 1xDMS-59 (2x DVI), SSD 2, 5" 180GB Intel® 535 series SATAIII 7mm, 19" IPC case do racku, 480mm hloubka, černý, Fortron FSP500-60GHN 80PLUS BRONZE, black, bulk 500W, MS Win Pro 8.1 Win64bit Czech 1pk OEM DVD, Výstupy na monitory, GK: 2x DVI

SW LATIS SQL s moduly:

- LGLE Konfigurace grafických dat (Latis graphic layer editor)
- LAT Nástroj pro správu (Latis administration tool)
- LOW Pracoviště operátora (Latis operation Workstation)
- LESI interface pro připojení EPS Esser
- LZTI interface pro připojení EPS Zettler
- Galaxy Smart interface pro připojení PZTS GALAXY
- Interface pro integraci SKV (vývoj)

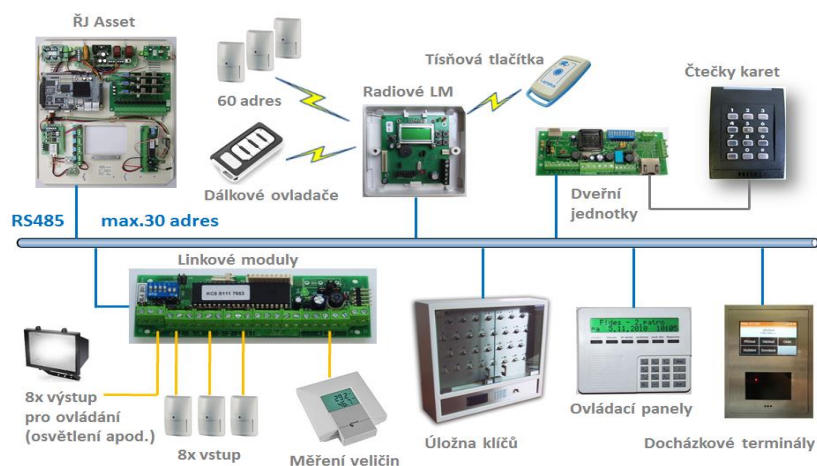
### 4.3 Návrh - Nová technologie

Vzhledem k instalovaným bezpečnostním technologiím a jejich reálné možnosti rozšíření především systému PZTS (pro pronájem laboratorních prostor, pronájem kanceláří, pronájem sportoviště) a s tím souvisejícím bezpečným provozem SKV, předkládám návrh řešení zabezpečení budovy prostřednictvím integrovaného systému PZTS a SKV.

#### 4.3.1 Popis technologie

Pro řešení zabezpečení budovy U5 integrovaným systémem PZTS a SKV jsem použil technologii ASSET českého výrobce a dodavatele f. TRADE Fides a.s. Tento systém je určen pro střední až velké objekty, je certifikován do stupně číslo 4, vysoké riziko dle NBU. Z hlediska technologie se jedná o modulární sběrniceový systém s podporou redundantního provozu řídicích jednotek. Řídicí jednotky pracují v prostředí stabilního operačního prostředí LINUX s možností vzdálené správy a údržby včetně možnosti aktualizace jejich firmwaru. Z hlediska PZTS lze k 12-ti komunikačním linkám systému, připojit až 360 modulů s 2872 vstupy, nebo 360 radiových modulů s 21600 bezdrátovými vstupy, nebo 360 dveřních jednotek pro dvě snímací zařízení (vstup/výstup - jedny dveře), nebo vzájemná kombinace uvedených možností.

Obrázek 16 Topologie Asset

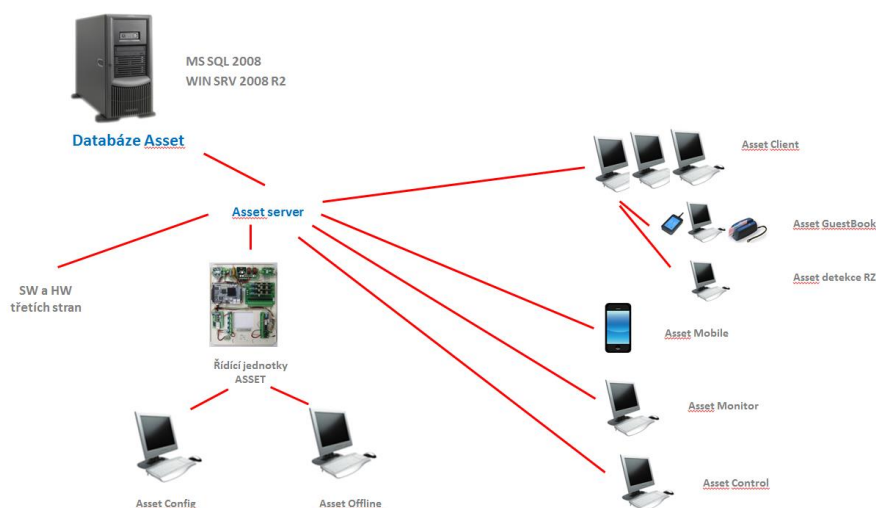


Zdroj: [37]

Z hlediska SKV jsou v systému zaintegrovány vybrané biometrické snímače. Dále systém podporuje kontrolu průchodů osob a jejich pohyb v objektu, docházku zaměstnanců, monitorování osob podle fotografií, ovládání dveří, výtahů, nebo turniketů, dále podporuje při-

pojení klíčových trezorů, klíčového hospodářství, řeší řízení parkoviště s možností rozeznání RZ vozidla, návštěvní knihu s možností připojit OCR čtečky dokladů. Poskytuje informace personálním systémům o docházce, účetním systémům o stravování, kopírování atd. Z hlediska Centrální správy je systém postaven na technologii klient – server a platformě Microsoft SQL. Systém podporuje standardní komunikační protokoly (AdemcoContact ID, Opentherm, BACnet) pro komunikaci s BMS. Při spojení s nadřazeným prvkem je využito šifrované komunikace AES-128 prostřednictvím komunikačního protokolu TCP IP. Z hlediska systému, služba ASSET Server podporuje integraci s ostatními systémy poskytnutím vývojové sady SDK, integraci do sítě BACnet nebo ostatními systémy (SAP, ANeT).

Obrázek 17 Topologie Asset server



Zdroj: [37]

Klientská aplikace ASSET Client zajišťuje jednoduchým ovládáním pro operátora pohodlnost při správě rozsáhlého systému. Lze ji nastavit dle konkrétních potřeb operátora a také pro operátora nastavit přístupová práva. Z klientské aplikace dle oprávnění operátora lze hromadně importovat a exportovat data, vyhledávat v historii, provádět plný audit, provádět potisk karet, spravovat uživatele. Velkou přidanou hodnotou systému je jednotná správa uživatelů pro systém PZTS a SKV. Klientská aplikace ve vazbě na systém CCTV obsahuje virtuální videomatici a umožňuje tak zobrazit uživatele při průchodu definovaným terminálem.



### 4.3.2 Technické řešení PZTS, SKV

V případě řešení s novou technologií a vzhledem k uvedeným vlastnostem nového systému bude možné využít stávající rozvody PZTS mezi detektory a linkovými moduly, rozvody komunikačních linek mezi ústřednou PZTS a linkovými moduly systému. Bude možné využít stávajícího umístění ústředny PZTS. Lze zachovat také množství, rozmístění a kapacitu napájecích zdrojů. Při volbě varianty linkových modulů s vyvážením 1kOhm, bude možné zachovat také koncové rezistory v jednotlivých detektorech a snížit tak časovou náročnost instalace. V případě zapojení více detektorů k jedné smyčce navrhuji doplnit pro každý detektor samostatnou smyčku, tzn. nárůst linkových modulů. Nově navrhovaný systém lze také využít pro monitorování fyzikálních vlastností (např. teplota, vlhkost) v serverovnách, laboratořích, PC učebnách. Systém okamžitě předá informaci přímo ostraže objektu, lze předejít značným škodám. Prvky potřebné pro přechod na novou technologii, která umožňuje popsané vlastnosti, jsou tak minimalizovány na linkové moduly, ovládací panely.

Jak bylo uvedeno vzhledem k snadno zneužitelnému formátu používaných karet a k získání možnosti jednotné správy uživatelů navrhuji přechod na karty se zabezpečením DESFire EV (13,56MHz). S tím dojde také ke změně stávajícího systému SKV. Nové snímací zařízení nahradí stávající prvky na stávajících místech. Stávající řídicí jednotky budou nahrazeny novými dveřními jednotkami tak aby vyhověly počtu obsluhovaných snímacích zařízení. Komunikace a napájení snímacího zařízení s dveřní jednotkou bude prostřednictvím stávající kabeláže. Komunikace dveřních jednotek s centrální řídicí jednotkou je standardně prostřednictvím rozhraní RS 485, Pro dodržení tohoto standardu bude nezbytné komunikační linku RS485 pro SKV vybudovat. Bude tak dodržena oddělená bezpečná komunikace modulů SKV mimo datovou síť. Místně bude možné využít některou z komunikačních linek s moduly PZTS. Napájení nových dveřních jednotek bude z nově instalovaných pomocných zálohovaných zdrojů, připojených ke stávajícím přívodům pro řídicí jednotky dosavadního systému. Kapacita zdrojů a doba zálohy bude navržena v souladu s ČSN EN 50131-1.

#### 4.3.2.1 Návrh prvků

Řídicí jednotky Asset 808, Linkové moduly LML8, Ovládací klávesnice KMU4, Dveřní jednotky Asset 10, Asset20. Pro přehledné vyhodnocení, ovládání bude nutno doplnit klientské pracoviště PC, monitory a SW aplikace. Ze stejného klientského pracoviště a stejné

aplikace je možné provádět nejen monitorování PZTS jak je uvedeno v kapitole 4. 3. 1. Popis technologie, ale také monitorovat provoz systému SKV.

#### **4.3.3 Integrovaný systém**

Návrh s novou technologií také plně podporuje nastavbový systém, který je uveden v kapitole 4.2.6. Zároveň je navrhovaný systém otevřený pro komunikaci se systémy třetích stran. Lze tak respektovat nestandardní požadavky, které běžné zabezpečovací systémy splnit nemohou. Otevřenost systému je garantována prostřednictvím webové služby, autorizace a autentizace klientské strany je řešena SSL certifikátem. Prostřednictvím otevřeného rozhraní je možné modifikovat běžné typy entit (identita, karta, heslo), ale také sledovat kompletní dění v celém aplikačním serveru. Veškeré změny perzistentních entit jsou okamžitě propagovány do koncových zařízení (ústředna PZTS) a jsou ihned platné. Otevřeností systému je kladen důraz na online funkce celého řešení. Pokud není možné např. z důvodu poruchy sítě požadavek zpracovat okamžitě, je na serveru uložen a ústředně je předán po obnově komunikace na síti. Je tak garantována konzistence celého řešení. V případě vzdálené správy nebo servisu je povolení přístupu řešeno např. autentizačním portálem (uživatel plně blokuje přístup technikovi, nelze se k ústředně přihlásit svým heslem). Pokud je potřeba provést servis, správce dočasně odblokuje přístup pomocí autentizačního portálu a technik se po omezenou dobu může přihlásit svým heslem k ústředně. K zesílení bezpečnosti je použito konceptu důvěryhodnosti serverů. Každé konkrétní řešení je podmíněno dohodou se správcem systémů.

#### **4.3.4 Rozvody, Kabeláž**

Rozvody budou provedeny podle odpovídajících obecně platných předpisů. Budou dodrženy zásady o úpravě rozvodných skříní, označování svorkovnic a kabelů, křížení a souběhu se silovým vedením. Páteřní rozvody budou uloženy převážně ve stávajících páteřních trasách v podhledu chodby. Kabeláž pro nové prvky bude uložena v samostatných ohebných trubkách na příchýtkách v podhledu, v technických prostorech budou nové trasy přisazeny na povrchu.

#### **4.3.5 Napájení**

Napájení slaboproudých systémů bude ze zálohovaných zdrojů malého napětí. Budou odpovídat požadavkům ČSN EN 50131-1 kapitola 9: „Každá část zařízení PZTS, která je napájena ze základního zdroje, musí při výpadku tohoto zdroje zůstat v časově omezeném

provozu z náhradního zdroje minimálně 30 hod. v pohotovostním stavu, z toho 15min. ve stavu poplachu, je-li výpadek signalizován v místě trvalé obsluhy“.

Servery, LAN switche a budou napojeny na síť 230V/50Hz a zálohovány UPS na dobu 30min. Klientské PC lokální UPS na dobu 5min.

#### **4.4 Realizace, uvedení do provozu, provoz, údržba**

Realizace uvedených systémů bude probíhat podle návrhu odsouhlasené realizační dokumentace. Realizace bude probíhat dodavatelským způsobem. Pracovníci realizační firmy budou prokazatelně oprávněni k montáži vybraných zařízení. Při provádění montážních prací bude nutné dodržet ustanovení vyhlášky Českého úřadu pro bezpečnost práce a českého báňského úřadu č.601/2006 Sb.. Jakékoliv změny musí být odsouhlaseny zástupcem investora, uživatele, bezpečnostního ředitele. Po ukončení montáže bude provedena kontrola potvrzující její kompletnost, případné odsouhlasené odchylky proti realizační dokumentaci budou zakresleny do dokumentace skutečného provedení. Budou provedeny všechny funkční zkoušky, po jejich ukončení bude provedena výchozí elektrická revize, která bude nedílnou součástí dokumentace skutečného provedení. Následně bude systém uveden do zkušebního provozu, během kterého se odstraní případné závady. Pak bude systém převeden do trvalého provozu.

Po celou dobu provozu bude správce systému povinen vést provozní knihy jednotlivých systémů. Zde budou provedeny veškeré záznamy o provozních stavech systému (vznik poplachové, poruchové události). Záznamy o provedených zkouškách systému. Oznámení poruch servisní organizaci, způsob a termín odstranění.

Se systémem bude předána dokumentace v rozsahu čl. 11 ČSN CLC TS 50131-7. Provoz, údržba a opravy se řídí články 12 a 13 téže normy.

##### **4.4.1 Návrh provozních předpisů**

Po převzetí systému do trvalého provozu vydá správce systémů místní předpisy pro běžný provoz, kontrolu a údržbu systému. Správce systémů zajistí proškolení a následné pravidelné přezkoušení pracovníků z těchto předpisů.

Příklad místních provozních předpisů:

- Instalované systémy je oprávněna obsluhovat pouze osoba určená a řádně proškolená správcem systémů.

- Všechny osoby přicházející do styku s instalovanými systémy jsou povinny dodržovat tyto zásady:
  - a. Při nástupu do zaměstnání vizuálně zkontrolovat úplnost a funkčnost systémů na svém pracovišti. Případné nedostatky neprodleně nahlásit správci systému, který zajistí opravu poškozených částí u servisní organizace a nedostatky zaznamená do provozní knihy.
  - b. Obsluhovat systém dle návodů k obsluze, případné nejasnosti konzultovat se správcem systému.
  - c. Znemožnit manipulaci a neodborný zásah do systémů třetím osobám.
  - d. Veškeré události (poplachu, poruchy, poškození,...) neprodleně hlásit správci systému.
  - e. Opravy a jakékoliv zásahy do SW i HW smí provádět pouze oprávněný pracovník servisní organizace v souladu se smlouvou o záručním pozáručním servisu.
- Pro správnou funkci systému je nutné udržovat všechny části systému v čistotě.

## 4.5 Návrh smlouvy

Důležitými prvky každé činnosti je vymezení pravidel, činností, podmínek a požadavků mezi objednatelem a zhotovitelem. Dále uvádím jako doporučení některé důležité prvky které musí být součástí smlouvy o dílo, servisní smlouvy.

### 4.5.1 Smlouva o dílo

1. Smluvní strany - Objednatel, Zhotovitel
  - sídlo, zastoupen, IČ, DIČ, zapsán u, bankovní spojení, kontaktní údaje
2. Předmět díla a jeho provádění
  - Dodávka a montáž...
  - Předané podklady - projektová dokumentace, stavební povolení
  - Rozsah díla - dle PD, která je jako nedílná součást smlouvy
  - Prohlášení zhotovitele, že předané podklady jsou vhodné k realizaci, že se seznámil s rozsahem díla a bude používat materiály a komponenty dle zákonných požadavků a ČSN (Zákon č.22/1997Sb.),
  - Změny rozsahu díla jen s dodatkem smlouvy.
  - Povinnost zhotovitele vést stavební deník a předkládat ho ke kontrole dle dohodnutých pravidel.

- Součást díla - zpracování dokumentace skutečného provedení, provedení revizních zkoušek, ostatních zkoušek, zaškolení zástupců objednatele, provedení zkušebního provozu, délka trvání, atd.

### 3. Místo a doba plnění, předání díla a záruka

- Místo plnění je...
- Termín předání, termín plnění dle harmonogramu
- Prohlášení zhotovitele, že nezjistil žádné překážky k provedení díla, zápis o převzetí staveniště.
- Zhotovitel bude respektovat pokyny objednatele, bude informovat o stavební nepřipravenosti.
- Zhotovitel bude dodržovat doporučení platných ČSN, ČSN EN, ČSN ISO.
- Zhotovitel poskytne záruku dle dohody, záruční doba začíná dnem od předání díla.

### 4. Cena za dílo

- Výše sjednané ceny dohodou, cena pevná
- Splatnost daňového dokladu
- Daňový doklad dle právních předpisů, se soupisem nainstalovaného materiálu a provedených prací
- Účtování DPH dle platných předpisů

### 5. Ostatní ujednání

- Zhotovitel zajistí předání vzniklých odpadů v souladu se zákonem o odpadech a ochraně přírody.
- Zhotovitel je povinen zajistit si pojištění odpovědnosti za škody způsobené jeho činností.
- Smluvní pokuty z prodlení za každý započatý den např. 0.5% z ceny díla
- Případy porušení smlouvy např. prodlení zhotovitele, prodlení s odstraněním nedostatků, ze strany objednatele neposkytnutí součinnosti, prodlení s úhradou díla.

### 6. Závěrečná ustanovení

- Počet vyhotovení smlouvy
- Součásti smlouvy např. Nabídka zhotovitele, Harmonogram prací

### 7. Datum a podpis zúčastněných stran.

### 8. Přílohy ke smlouvě

V případě, že součástí předmětu díla jsou softwarové produkty nebo SW licence, je důležité prostřednictvím přílohy smlouvy sjednat „LICENČNÍ UJEDNÁNÍ“ které vymezuje práva a povinnosti uživatele SW

- SW je vlastnictvím poskytovatele a je chráněn dohodami o autorských právech a duševním vlastnictví
- Časově omezená / neomezená licence
- Výslovný zákaz / nebo písemný souhlas s rozmnožováním SW a poskytováním licenčních čísel třetím stranám
- Způsob poskytování upgradu SW
- Ujednání o sankcích při porušení licenčního ujednání
- Souhlasné prohlášení uživatele s podmínkami

#### 4.5.2 Servisní smlouva

Ve smlouvě o poskytování servisních služeb je nutno následující.

1. Smluvní strany - Objednatel, Zhotovitel
  - sídlo, zastoupen, IČ, DIČ, zapsán u, bankovní spojení, kontaktní údaje
2. Předmět smlouvy
  - Závazek zhotovitele poskytovat servis bezpečnostních technologií v provozuschopném stavu a zajišťovat provozuschopnost.
  - Místo plnění v objektu / objektech...
3. Rozsah a termíny plnění
  - Revize bezpečnostního systému - vypracovat a předat revizní zprávu 1x ročně ve dvou vyhotoveních
  - Pravidelné prohlídky bezpečnostního systému - vypracovat a předat zprávu o provedené pravidelné prohlídce
  - Opravy a údržba bezpečnostního systému - na základě objednávky na uvedené kontakty ..... Závazek zhotovitele dle dohodnutých podmínek, nástupní lhůta od ohlášení závady.
  - Ostatní servisní služby - preventivní prohlídky, konzultace, programátorské práce, příprava nabídky

O každé z činností je povinnost provést zápis do provozních knih bezpečnostních systémů.

4. Cena a platební podmínky

- Cena za revize bezpečnostního systému
- Cena za pravidelné prohlídky bezpečnostního systému
- Cena za opravy a údržbu bezpečnostního systému
- Cena za ostatní servisní služby

Ceny dohodnuty dle přiloženého ceníku služeb, prací, materiálu

- Zhotovitel bude respektovat pokyny objednatele, bude informovat o stavební nepřipravenosti.
- Zhotovitel bude dodržovat doporučení platných ČSN, ČSN EN, ČSN ISO.
- Zhotovitel poskytne záruku dle dohody, záruční doba začíná dnem od předání díla.

5. Povinnosti objednatele např.:

- Umožnění přístupu k místu kde je instalován systém
- Umožnění bezproblémového vykonání servisu, prohlídky, revize
- Zajistit proškolení koncových uživatelů
- Opatřením znemožnit zásah do systému třetí osobou
- Řádně a včas hradit sjednanou cenu

6. Povinnosti zhotovitele např.:

- Zachovávat mlčenlivost o všech skutečnostech, které se týkají bezpečnostních systémů v objektu
- Poskytovat plnění smlouvy dle dohodnutých podmínek
- Při plnění smlouvy postupovat s odbornou péčí dle platných doporučení ČSN, ČSN EN, ČSN ISO.
- Před vstupem do objektu za účelem plnění předmětu smlouvy uvědomit uživatele.

7. Doba trvání smlouvy a její ukončení

- Smlouva na dobu určitou / neurčitou
- V případě ukončení smlouvy výpovědní lhůta např. 3měsíce
- Oprávnění odstoupení od smlouvy
- Provedení odstoupení od smlouvy

8. Smluvní pokuty

- V případě objednatele s úhradou
- V případě zhotovitele se zahájením opravy

9. Všeobecná ustanovení např.:

- Zachování mlčenlivosti v souvislosti se smlouvou
- Právní vztahy se řídí ustanoveními občanského zákoníku
- Vyhotovení smlouvy ve dvou provedení
- Prohlášení obou stran o seznámení s obsahem smlouvy

10. Datum a podpis zúčastněných stran.



## 5 ROZVAHA

Doplnění bezpečnostních systémů v navrženém rozsahu respektuje požadavky uvedené v metodických pokynech k zajištění bezpečnosti a ochrany zdraví dětí žáků a studentů ve školách a školských zařízeních, které jsou zřizované ministerstvem školství mládeže a tělovýchovy a zároveň požadavky na stupeň zabezpečení dle doporučení z Asociace Grémium Alarm. Na základě navrženého technického řešení jsem oslovil dodavatelské organizace s požadavkem o cenovou kalkulaci technologií a realizační firmu o kalkulaci montážních prací. Zde uvádím celkovou cenovou rekapitulaci předpokládaných dodavatelských a montážních činností podle technologií. Každou technologii lze s částečnou modifikací realizovat jako samostatnou etapu.

### 5.1 Rekapitulace

#### 5.1.1 Rekapitulace dle technologií

Tabulka 5 Rekapitulace rozpočtu dle technologií

<b>Rozpočet</b>			
	<b>Přístupové systémy</b>	<b>Dodávky</b>	<b>Montáže</b>
		<b>978 136,34 Kč</b>	<b>119 594,00 Kč</b>
<b>DPH: DPH 21%</b>		<b>205 408,50 Kč</b>	<b>25 114,50 Kč</b>
<b>Celkem</b>		<b>1 183 544,84 Kč</b>	<b>144 709,50 Kč</b>
	<b>CELKEM</b>	<b>1 328 254,34 Kč</b>	
	<b>PZTS</b>	<b>Dodávky</b>	<b>Montáže</b>
		<b>195 428,88 Kč</b>	<b>109 968,00 Kč</b>
<b>DPH: DPH 21%</b>		<b>41 040,00 Kč</b>	<b>23 093,50 Kč</b>
<b>Celkem</b>		<b>236 468,88 Kč</b>	<b>133 061,50 Kč</b>
	<b>CELKEM</b>	<b>369 530,38 Kč</b>	
	<b>CCTV</b>	<b>Dodávky</b>	<b>Montáže</b>
		<b>1 395 245,82 Kč</b>	<b>98 821,00 Kč</b>
<b>DPH: DPH 21%</b>		<b>293 001,50 Kč</b>	<b>20 752,50 Kč</b>
<b>Celkem</b>		<b>1 688 247,32 Kč</b>	<b>119 573,50 Kč</b>
	<b>CELKEM</b>	<b>1 807 820,82 Kč</b>	

	<b>Grafická Nástavba LATIS</b>	<b>Dodávky</b>	<b>Montáže</b>
		<b>241 669,00 Kč</b>	<b>94 901,00 Kč</b>
<b>DPH: DPH 21%</b>		<b>50 750,50 Kč</b>	<b>19 929,00 Kč</b>
<b>Celkem</b>		<b>292 419,50 Kč</b>	<b>114 830,00 Kč</b>
	<b>CELKEM</b>	<b>407 249,50 Kč</b>	
	<b>Hlavní trasa</b>	<b>Dodávky</b>	<b>Montáže</b>
		<b>49 104,06 Kč</b>	<b>65 523,00 Kč</b>
<b>DPH: DPH 21%</b>		<b>10 312,00 Kč</b>	<b>13 760,00 Kč</b>
<b>Celkem</b>		<b>59 416,06 Kč</b>	<b>79 293,00 Kč</b>
	<b>CELKEM</b>	<b>138 699,06 Kč</b>	
	<b>Výměna technologie</b>	<b>Dodávky</b>	<b>Montáže</b>
		<b>800 479,50 Kč</b>	<b>109 535,00 Kč</b>
<b>DPH: DPH 21%</b>		<b>168 100,50 Kč</b>	<b>23 002,50 Kč</b>
<b>Celkem</b>		<b>968 580,00 Kč</b>	<b>132 537,50 Kč</b>
	<b>CELKEM</b>	<b>1 101 117,50 Kč</b>	
	<b>Ostatní služby</b>		
	<b>Celkem</b>		<b>248 550,00 Kč</b>
<b>DPH: DPH 21%</b>			<b>52 195,50 Kč</b>
	<b>CELKEM</b>	<b>300 745,50 Kč</b>	

Zdroj: Autor

V části „Výměna technologie“ je započítána výměna stávajícího přístupového systému. Kalkulace pro systém PZTS zde zahrnuta není. V položkovém rozpočtu je uvedena orientační cena nových linkových modulů a nových ovládacích klávesnic. Výsledná cena i při výměně technologie PZTS bude navýšena podle konkrétních počtů potřebných zařízení.

## Rekapitulace rozpočtu

Tabulka 6 Rekapitulace rozpočtu

<b>Rekapitulace rozpočtu</b>			
Základní rozpočtové náklady			
Materiál a dodávky celkem			3 660 063,60 Kč
Montážní práce a služby celkem			598 342,00 Kč
Ostatní			248 550,00 Kč
<b>Celkem</b>			<b>4 506 955,60 Kč</b>
<b>Celkem bez DPH (zaokrouhleno)</b>			<b>4 506 955,60 Kč</b>
<b>Daň z přidané hodnoty</b>			
DPH 21%	%	4506955,6	946 460,68 Kč
<b>Suma DPH</b>			<b>946 460,68 Kč</b>
<b>DPH Celkem (zaokrouhleno)</b>			<b>946 460,50 Kč</b>
<b>Celkem s DPH</b>			<b>5 453 416,10 Kč</b>

Zdroj: Autor

## 5.2 Možné způsoby financování

### 5.2.1 Dotační programy MŠMT ČR

V popsáném rozsahu a objemu technického řešení se může jednat o investiční záměr. Rozhodnutí o realizaci investičního záměru musí být nejen na základě např. odhadu budoucích výhod záměru, provozních nákladech záměru, ale také způsobech financování. Rozhodnutí o realizaci záměru se pak musí projevit v navýšení investičního rozpočtu v hospodaření subjektu pro daný rok. Financování investic je možné několika způsoby: z investičních a dotačních programů MŠMT ČR, MF ČR, dotačních programů na financování z EU. Na financování záměru pro školu zřizovanou státem je možné využít finančních prostředků poskytovaných ministerstvem školství jako dotaci veřejným vysokým školám. MŠMT pravidelně zveřejňuje pravidla pro její čerpání.

### 5.2.2 Dotační programy MMR ČR

Prostřednictvím Ministerstva pro místní rozvoj ČR lze využít Evropský fond pro regionální rozvoj (EFRR/ERDF), který se zaměřuje na investiční (infrastrukturní) projekty, modernizaci, výstavbu nebo opravy.

### 5.2.3 Dotační programy MF ČR

Dále prostřednictvím ministerstva financí ČR, které je Národním kontaktním místem a je zodpovědné za řízení finančních mechanismů EHP / Norska v České republice.

### 5.2.4 Financování jako službu

Další a často využívaný způsob financování je prostřednictvím tzv. partnerství veřejného a soukromého sektoru. Společnosti nabízejí řešení financování vybraných projektů formou služby. Služba je založena vzájemném smluvním vztahu mezi poskytovatelem a zadavatelem. Jsou stanoveny podmínky realizace projektu, záruky (např. víceletá na použitý materiál), revize a servisu (např. 24 servisní pohotovost), obnovy zařízení (např. průběžná obnova). U tohoto řešení je za spolehlivý provoz všech technických prostředků zodpovědný poskytovatel služby. To je jen jedna z výhod řešení formou služby, dále šetří jednorázové vynaložení finančních prostředků investičního charakteru. Financování je řešeno pravidelnou úhradou (např. měsíční) která může být hrazena z provozních nákladů. Další výhodou je pravidelná údržba a servis včetně průběžné obnovy zařízení upgradu SW. Taková řešení jsou nejvhodnější v případech rekonstrukce celého systémů.

## 5.3 Doporučený postup výstavby

- Vybudování hlavní trasy
- Doplnění přístupového systému
- Doplnění CCTV
- Doplnění PZTS
- Integrace systémů

## 6 ZÁVĚR

Teoretická práce se věnuje problematice zabezpečení školních budov v ČR obecně. Autor čerpal informace z tuzemské literatury, legislativních předpisů, metodických doporučení a statistik policie ČR. Poznatky byly využity v praktické části práce. Hlavním cílem byl návrh technického řešení na zlepšení zabezpečení budovy U5 ve vztahu k průchodu osob. Ke splnění tohoto úkolu bylo třeba splnit několik dílčích cílů. Dílčími cíli byla – analýza budovy a jejího okolí, analýza současného stavu zabezpečení budovy včetně jejího vyhodnocení a volba optimálního řešení.

Analýza budovy prokázala, že se jedná o moderně rekonstruovanou budovu včetně moderních technologických zařízení. Přestože z hlediska zabezpečení lze říci, že každá budova je stejná, prokázalo se, že svou polohou a členěním je tato budova specifická. Bylo nutné při řešení přihlídnout k odlišnostem.

Analýza současného stavu zabezpečení prokázala, že instalované technologie jsou plně funkční, svými technickými parametry odpovídají době instalace. Bylo zjištěno, že v případě požadavku na rozšíření systémů může dojít k naplnění kapacity instalovaného zařízení. Dále bylo zjištěno, že nelze splnit požadavek na jednotnou správu uživatelů různých systémů z jednoho pracovního prostředí. Případně nelze vyhovět požadavku na možnost propagace uživatelů v systémech třetích stran.

Na základě zjištění z analýz byly v praktické části této práce zpracovány návrhy technických řešení podle jednotlivých technologií. Konkrétně doplněním stávajících bezpečnostních technologií s možností integrace do nastavbového a grafického systému prostřednictvím komunikačních rozhraní a nové páteřní trasy prostřednictvím kabelů s optickými vlákny. Pro možnost srovnání byl vytvořen návrh technického řešení systémem, který umožňuje svými parametry kompletní zabezpečení budovy a to s jednotnou dálkovou správou uživatelů. Svými parametry splňuje moderní standard současných technologií.

Cílem bylo navrhnout řešení, které podá pomocnou ruku pracovníkům fyzické ostrahy vzhledem k přehlednosti předkládaných poplachových a provozních informací. Toto řešení pak svými technickými parametry splní požadavky na spolehlivý provoz, komunikaci s aplikacemi třetích stran a širokou možnost rozšíření do budoucnosti. Celkové řešení včetně doplnění systému PZTS, CCTV a usnadnění přístupu zásahu přispěje k vyššímu standardu zabezpečení studentů a zaměstnanců univerzity.

## SEZNAM POUŽITÉ LITERATURY

1. MORKES, František. Archiv: Největší reforma školství v dějinách, 230. výročí Všeobecného školního řádu. *Učitelské noviny*. [Online] Diversite, 2004. [Citace: 16. duben 2016.] <http://www.ucitelskenoviny.cz/?archiv&clanek=4731>.
2. ČR, Policie. Policie: Úvodní strana: Informační servis: Statistiky: Kriminalita. *Policie ČR*. [Online] 2015. [Citace: 28. Únor 2016.] <http://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2015.aspx>.
3. FIDRMUC, Jaroslav. msmt.cz/dokumenty. *MŠMT*. [Online] 2016. [Citace: 17. duben 2016.] <http://www.msmt.cz/dokumenty/metodicky-pokyn-k-zajisteni-bezpecnosti-a-ochrany-zdravi-deti-zaku-a-studentu-ve-skolach-a-skolskych-zarizenich-zrizovanych-ministerstvem-skolstvi-mladeze-a-telovychovy>.
4. LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. 1. Zlín : VeRBuM, 2011. str. 316. 978-8087500-05-7.
5. URBAN, Miroslav, MERHAUT, Jan a KALEVIČOVÁ, Eva. ČSN EN 60839-11-1. *Poplachové a elektronické bezpečnostní systémy- část 11-1: Elektronické systémy kontroly vstupu- Požadavky na systém a komponenty*. Praha : ÚNMZ, 2014.
6. ŠTĚTINA, Kamil, a KYNCL, Tomáš. Úvod do přístupových systémů. *adiglobal. produkty*. [Online] 2016. [Citace: 18. duben 2016.] <http://www.adi-olympo.cz>.
7. STANĚK, Jan, a ŘEHÁK, Jan. RS 485 & 422. *vyvoj.hw.cz*. [Online] HW server s r.o., 2014. [Citace: 19. duben 2016.] <http://vyvoj.hw.cz/teorie-a-praxe/dokumentace/rs-485-422.html>.
8. *Access a key distribution management*. GAŠPARÍK, Petr. 1, Praha : IDG Czech Republic a.s., 2015. 1210-9924.
9. *Identitymanagement zjednoduší správu uživatelských účtů*. LÍZNER, Martin. 1, Praha : Security World, 2010, Security World.
10. ŠREJBER, Jan. HiCo nebo LoCo magnetické karty? *Cardhouse, blog*. [Online] COPYSCAPE, 2012. [Citace: 20. duben 2016.] <http://cardhouse.cz/cs/blog/hico-nebo-loco-magneticke-karty>.

11. Elektronik, EBV. download: elecfreaks. *elecfreaks*. [Online] 2010. [Citace: 21. duben 2016.] [http://elecfreaks.com/store/download/datasheet/NFC/rfid\\_guide.pdf](http://elecfreaks.com/store/download/datasheet/NFC/rfid_guide.pdf).
12. UHLÁŘ, Jan. *Technická ochrana objektů*. Praha : PA ČR, 2005. str. 229. 8072511890.
13. *Biometrické metody identifikace osob v bezpečnostní praxi*. ŠČUREK, Radomír. Ostrava : VŠB TU Ostrava, 2008, str. 58.
14. KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Blatná : cricetus, 2003. 80-902938-2-4.
15. LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I*. Zlín : Univerzita Tomáše Bati, Fakulta technologická, 2003. 8073181193.
16. ČSN EN 50131-1 ed.2 Poplachové zabezpečovací a tísňové systémy - část 1 Systémové požadavky.
17. Information and communications technology strategic plan. *University of Oxford*. [Online] PRAC, 2007. <http://www.ict.ox.ac.uk/strategy/plan/plan.xml.ID=appF>.
18. ROUSE, Margaret. What is identity management (ID management) ? - Definition from WhatIs.com. *Search Security*. [Online] Tech Target, 2000-2016. <http://searchsecurity.techtarget.com/definition/identity-management-ID-management>.
19. SEMANČÍK, Radovan. IT Systems. *Cesta k efektivnímu identity managementu*. [Online] 6 2015. <http://m.systemonline.cz/sprava-it/cesta-k-efektivnimu-idm-architektura-iam-reseni.htm>.
20. LEJSEK, Zdeněk. Správa identit a řízení přístupu s ESB. [editor] Grásgruber a Lukáš. *IT Systems*. 14, 2012, Sv. 10/2012.
21. OVH.cz. *Jak funguje certifikát SSL*. [Online] Jak funguje certifikát SSL.
22. *Projektování bezpečnostních systémů*. VALOUCH, Jan. 1, Zlín : Univerzita Tomáše Bati ve Zlíně, 2012. 978-80-7454-230-5.
23. UNMZ. Seznam ČSN. *Vyhledávání / Seznam ČSN*. [Online] [Citace: 20. březen 2016.] <http://seznamcsn.unmz.cz/>.
24. HOLAS, Milan a JURAČKA, Zdeněk. ČSN EN 50133-1. *Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - část 1: Systémové požadavky*. Praha : Český normalizační institut, 2001.

25. Polachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 7 pokyny pro aplikace. Praha : UNMZ, 2011. 334591.
26. UNMZ. ČSN CLC/TS 50398. *Poplachové systémy - Kombinované a integrované systémy - Všeobecné požadavky*. Praha : UNMZ, 2009.
27. UTB Zlín UTB, struktura, dislokace - budov. *UTB, struktura, dislokace - budov*. [Online] [http://www.utb.cz/struktura/dislokace - budov](http://www.utb.cz/struktura/dislokace-budov).
28. ADIGlobal *ADI, Produkty*. [Online] [https://www.adiglobal.cz/iWWW/cz/produkty110.nsf/web\\_category\\_list1](https://www.adiglobal.cz/iWWW/cz/produkty110.nsf/web_category_list1).
29. Cominfo trade, a.s. *Cominfo, produkty*. [Online] <http://www.cominfo-trade.com/cz/produkty/>.
30. *Husky M30/M50 Administration manual*. MILESTONE.
31. EPS PRAHA. *Eps Praha, fotoalbum, elektická požární signalizace, Zettler*. [Online] <http://www.epspraha.cz/fotoalbum/elektricka-pozarni-signalizace/-EPS-Zettler>.
32. Axis. *Instalační manuál True View Report*. [Online]
33. Metel sr.o. *AXIS, Mete, produkty*. [Online] <https://www.metel.eu/produkty/reseni?categoryId=115>.
34. TSS group. *TSS, produkty, SONY*. [Online] <http://www.tssgroup.cz/sony-snc-eb632r-kompaktni-ip-kamera/#ke-stazeni>.
35. *Provozování kamerových systémů*. ÚOOZ. Praha : Úřad pro ochranu osobních údajů, 2012. 978-80210-6017-3.
36. Trade FIDES a.s. *Katalogový list LATIS*. [Online]
37. Trade FIDES a.s. *Katalogový list ASSET*. [Online]
38. URBAN, Miroslav a MERHAUT, Jan. ČSN EN 60839-11-1. Poplachové a elektronické bezpečnostní systémy část 11-1: Elektronické systémy kontroly vstupu - Požadavky na systém a komponenty. Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.
39. UNMZ/ Povinné informace. UNMZ. [Online] [code i-servis.cz](http://www.unmz.cz/test/povinne-informace), 2016. [Citace: 30. březen 2016.] <http://www.unmz.cz/test/povinne-informace>.



**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

DPPC, ARC	Poplachové přijímací dohledové centrum (Alarm Reciving Centre)
I&HAS	Poplachový zabezpečovací a tísňový systém (Intrusion and Hold-up Alarm System)
PIN	Osobní identifikační číslo (Personal Identification Number)
PC	Osobní počítač (Personal Computer)
USB	Universální sériová sběrnice (Universal Serial Bus)
LAN	Lokální síť počítačů (Local Area Network)
SQL	Standardizovaný strukturovaný dotazovací jazyk (Structured Query Language)
TCP/IP	Primární přenosový protokol/ protokol síťové vrstvy (Transmission Control Protocol/Internet Protocol)
MFA	Více faktorová autentizace (Multi Factor Authentication)
IDM	Správa Identit (Identity Management)
ATZ	Zdvojené zapojení zón (Advanced Technology Zoning)
ICT	Informační a komunikační technologie (Information and Comunication Technologies)
LDV	Zařízení nízkého napětí (Low Voltage Diferential)
EMC	Elektro magnetická kompatibilita (Electro Magnetic Compatibility)
EPS	Elektrická požární signalizace
BT	Bezpečnostní třída
SBS	Soukromá bezpečnostní služba
OCR	Optické rozpoznání znaků ( Optical Character Recognition)
SDK	Vývojová sada nástrojů (Software Development kit)
DES	Symetrický šifrovací algoritmus (Data Encryption Standard)

**SEZNAM OBRÁZKŮ**

Obrázek 1	Sběrníková topologie.....	16
Obrázek 2	MFA Vícefaktorová autentizace .....	18
Obrázek 3	PZTS Drátové prvky - PZTS Ústředna .....	26
Obrázek 4	Architektura IDM.....	30
Obrázek 5	SSL/TLS komunikace .....	31
Obrázek 6	Situace U5 .....	42
Obrázek 7	Ovládací panel PZTS GALAXY-MK7 .....	45
Obrázek 8	Snímací prvek Comifo L-PRO, L-PRO/K .....	46
Obrázek 9	CCTV Klientské pracoviště .....	47
Obrázek 10	EPS LOOP 500 Kruhové vedení.....	49
Obrázek 11	People counter .....	55
Obrázek 12	Topologie LAN RING .....	56
Obrázek 13	CCTV Kamera s IR Přísvitem (kompakt).....	58
Obrázek 14	Grafické znázornění integrace PZTS, EPS .....	61
Obrázek 15	Pracoviště operátora LOW .....	62
Obrázek 16	Topologie Asset .....	63
Obrázek 17	Topologie Asset server.....	64

**SEZNAM TABULEK**

Tabulka 1	Role .....	18
Tabulka 2	Stupně zabezpečení PZTS .....	37
Tabulka 3	Třídy prostředí .....	38
Tabulka 4	Statistika krádeží vloupání do škol .....	43
Tabulka 5	Rekapitulace rozpočtu dle technologií .....	73
Tabulka 6	Rekapitulace rozpočtu .....	75

**SEZNAM PŘÍLOH**

Příloha 1	Položkový rozpočet
Příloha 2	Výkres č.01 – Doplnění zabezpečení U5 - 1.NP (CD)
Příloha 3	Výkres č.02 - Doplnění zabezpečení U5 - 2.NP (CD)
Příloha 4	Výkres č.03 – Doplnění zabezpečení U5 – 3.NP (CD)
Příloha 5	Výkres č.04 – Doplnění zabezpečení U5 – 4.NP (CD)
Příloha 6	Výkres č.05 – Doplnění zabezpečení U5 – 5.NP (CD)
Příloha 7	Výkres č.06 – Doplnění zabezpečení U5 – 6.NP (CD)
Příloha 8	Výkres č.07 – Doplnění zabezpečení U5 – 7.NP (CD)

Zakázkové č:

***Doplnění zabezpečení\_přístupový systém U5 Zlín***

Rozpočet č: ZH01686

**Platnost nabídky 3 měsíce od data vystavení**

Rekapitulace rozpočtu					
HLAVA III.	Základní rozpočtové náklady				
	Materiál a dodávky celkem			3 660 063,60 Kč	
	Montážní práce a služby celkem			598 342,00 Kč	
	Ostatní			248 550,00 Kč	
	Celkem			4 506 955,60 Kč	
Celkem bez DPH (zaokrouhleno)				4 506 955,60 Kč	
Daň z přidané hodnoty					
DPH 21%		21	%	4506955,6	946 460,68 Kč
Suma DPH					946 460,68 Kč
DPH Celkem (zaokrouhleno)					946 460,50 Kč
Celkem s DPH					5 453 416,10 Kč

	<b>Rozpočet</b>				
	<b>Dodávky, Přístupové systémy</b>				
Číslo položky	Popis položky	Počet	MJ	Jedn. cena	Celkem
	REA-MP elektronika snímače bez klávesnice bez display, vč zdroje	5	ks	19 299,00 Kč	96 495,00 Kč
PBQ12150	PBQ12150 Akumulátor 12V / 18Ah VdS	10	ks	1 404,00 Kč	14 040,00 Kč
	L-PRO/K čtecí hlava s klávesnicí 2x LED čtení do 6 cm	16	ks	8 742,00 Kč	139 872,00 Kč
MC2110C	MC2110C MG kontakt čtyřdrátový s úhelníkem a pracovní mezerou	13	ks	317,00 Kč	4 121,00 Kč
RKZ111	RKZ111 Plastová nízká propojovací krabice, 7+1 pájecích svor	9	ks	240,00 Kč	2 160,00 Kč
	Průmyslový switch 2G-2S-1.4.1 BOX PoE+	4	ks	27 500,00 Kč	110 000,00 Kč
	miniGBIC SFP SC/WDM 1000 Base	8	ks	682,70 Kč	5 461,60 Kč
P05D-SCSC-02	P05D-SCSC-02 Patch kabel KELine SC - SC Duplex 50/125 OM2 2	16	ks	138,32 Kč	2 213,12 Kč
KEL-C5E-T-015	KEL-C5E-T-015 Patch kabel KELine Giga 2xRJ45 Cat.5E S/FTP L	10	ks	21,06 Kč	210,60 Kč
AXIS 209-FD-R	AXIS 209-FD-R Speciální WEB kamera do dopravních prostředků	2	ks	13 400,00 Kč	26 800,00 Kč
		0		0,00 Kč	0,00 Kč
383007225	VODIC SFTP CAT5E FRNC 4x2xAWG24	675	m	14,18 Kč	9 571,50 Kč
CYKY-O 3x1,5 BU	CYKY-O 3x1,5 BUBEN Kabel CYKY-O 3x 1,5 buben	140	m	12,49 Kč	1 748,60 Kč
CYKY-J 3x2,5 KR	CYKY-J 3x2,5 KRUH Kabel CYKY-J 3x 2,5 /100m	140	m	17,58 Kč	2 461,20 Kč
J-Y(St)Y 2x2x0,8	J-Y(St)Y 2x2x0,8 rudá Kabel J-Y(St)Y 2x2x0,8 rudá	190	m	6,68 Kč	1 269,20 Kč
2325/LPE-1	2325/LPE-1TRUBKA OHEBNA 320N	190	m	9,04 Kč	1 717,60 Kč
8,59506E+12	8595057610170 Lišta vkladací 40x 20 bílá LHD 2m	32	m	21,16 Kč	677,12 Kč
2153130	2153130 Přichytka MULTI-QUICK 25-28,5 2153130	380	ks	4,96 Kč	1 884,80 Kč
		0		0,00 Kč	0,00 Kč
	Turniket venkovní provedení nerez	1	ks	135 000,00 Kč	135 000,00 Kč
	Turniket vnitřní trnový BAR ST komaxit	1	ks	58 000,00 Kč	58 000,00 Kč
	Konstrukce zábran BAR-BA výška 1,6 m skleněná výplň	10	ks	15 600,00 Kč	156 000,00 Kč
	Branka otevírací s přídržným elektromagnetem výplň sklo	3	ks	55 311,00 Kč	165 933,00 Kč
	<b>Celkem</b>				<b>978 136,34 Kč</b>
<b>DPH:</b>	<b>DPH 21%</b>				<b>205 408,50 Kč</b>
	<b>Montáže, Přístupové systémy</b>				
Číslo položky	Popis položky	Počet	MJ	Jedn. cena	Celkem
XACS-M00070	Montáž rozvodného členu	5	ks	350,00 Kč	1 750,00 Kč
XM-ZDR-00040	Instalace akumulátoru	10	ks	117,00 Kč	1 170,00 Kč
XACS-M00080	Montáž čtečky	16	ks	250,00 Kč	4 000,00 Kč

XACS-M00020	Oživení systému náklady na 1 čtečku	16	ks	117,00 Kč	1 872,00 Kč
XM-EZS-00120	Montáž magnetického kontaktu kov	13	ks	233,00 Kč	3 029,00 Kč
XM-EZS-00070	Montáž a zapojení propojovací krabice s OK	9	ks	233,00 Kč	2 097,00 Kč
XM-STK-00240	Instalace akt. prvku bez managementu	4	ks	175,00 Kč	700,00 Kč
XM-STK-00140	Instalace Patch kabelu	26	ks	9,00 Kč	234,00 Kč
XACS-M00050	Instalace a konfigurace přístupu - hodi- nově	10	hod	500,00 Kč	5 000,00 Kč
XCTV-M000020	Instalace kamery	2	ks	850,00 Kč	1 700,00 Kč
XCTV-M000260	Instalace SW na PC	6	hod	500,00 Kč	3 000,00 Kč
XCTV-M000230	Programování uživatelských požadavků	16	hod	500,00 Kč	8 000,00 Kč
XM-KAB-00020	Kabel do 10mm v trub.,liště	1145	m	12,00 Kč	13 740,00 Kč
XM-KAB-00290	Trubka PVC na om. vč. přích.	190	m	41,00 Kč	7 790,00 Kč
XM-KAB-00330	Elinstal. lišta do LV 40	32	m	41,00 Kč	1 312,00 Kč
	Přípravné stavební práce	1	kpl	19 200,00 Kč	19 200,00 Kč
	Koordinační práce turniket	1	kpl	6 500,00 Kč	6 500,00 Kč
	Instalace turniketu, mechanických zá- bran	1	kpl	33 500,00 Kč	33 500,00 Kč
XM-EZS-00230	Programování základních parametrů ústř.	10	hod	500,00 Kč	5 000,00 Kč
	<b>Celkem</b>				<b>119 594,00 Kč</b>
<b>DPH:</b>	<b>DPH 21%</b>				<b>25 114,50 Kč</b>
	<b>Dodávky PZTS</b>				
Číslo položky	Popis položky	Počet	MJ	Jedn. cena	Celkem
G8	G8 Koncentrátor v kovovém krytu pro 8 zón a 4 PGM výstupy	14	ks	3 643,00 Kč	51 002,00 Kč
AXSP K40/5A	AXSP K40/5A Spínaný zdroj v kovovém krytu 13,8 Vss / 5A s v	7	ks	5 550,00 Kč	38 850,00 Kč
PBQ12240	PBQ12240 Akumulátor 12V / 26Ah VdS	7	ks	1 805,00 Kč	12 635,00 Kč
PB2	PB2 ART 476 tísňové tlač. bílé s ochr. odklápěcím krytem	33	ks	680,00 Kč	22 440,00 Kč
	FAP 3002 tahový snímač	16	ks	1 150,00 Kč	18 400,00 Kč
	NICE klíčový spínač	8	ks	650,00 Kč	5 200,00 Kč
	Tlačítko ABB přivolání asistence, bloka- ce, otevření	4	ks	428,00 Kč	1 712,00 Kč
RKZ111	RKZ111 Plastová nízká propojovací krabice, 7+1 pájecích svor	10	ks	240,00 Kč	2 400,00 Kč
ART1490BZ	ART1490BZ Signalizační velká červená LED dioda v krytu s bzu	1	ks	299,00 Kč	299,00 Kč
		0		0,00 Kč	0,00 Kč
383007225	VODIC SFTP CAT5E FRNC 4x2xAWG24	875	m	14,18 Kč	12 407,50 Kč
CYKY-O 3x1,5 BU	CYKY-O 3x1,5 BUBEN Kabel CYKY-O 3x 1,5 buben	340	m	12,49 Kč	4 246,60 Kč
	CYSY 2x1	765	m	9,50 Kč	7 267,50 Kč
SYKFY 3x2x0,5 K	SYKFY 3x2x0,5 KRUH Kabel SYKFY 3x2x0,5 kruh	1850	m	6,44 Kč	11 914,00 Kč
2325/LPE-1	2325/LPE-1TRUBKA OHEBNA 320N	460	m	9,04 Kč	4 158,40 Kč
8,59506E+12	8595057610170 Lišta vkladací 40x 20 bílá LHD 2m	118	m	21,16 Kč	2 496,88 Kč

	<b>Celkem</b>				<b>195 428,88 Kč</b>
<b>DPH:</b>	<b>DPH 21%</b>				<b>41 040,00 Kč</b>
	<b>Montáže PZTS</b>				
Číslo položky	Popis položky	Počet	MJ	Jedn. cena	Celkem
XM-EZS-00050	Montáž expanderu	14	ks	700,00 Kč	9 800,00 Kč
XM-ZDR-00010	Montáž zdroje s dobíječem v OC skříni	7	ks	525,00 Kč	3 675,00 Kč
XM-ZDR-00040	Instalace akumulátoru	7	ks	117,00 Kč	819,00 Kč
XM-EZS-00170	Montáž tísňového hlásiče	49	ks	175,00 Kč	8 575,00 Kč
XM-EZS-00160	Montáž klíčového spínače, talčítka	12	ks	408,00 Kč	4 896,00 Kč
XM-EZS-00070	Montáž a zapojení propojovací krabice s OK	10	ks	233,00 Kč	2 330,00 Kč
XM-EZS-00170	Montáž opticko akustické signalizace	1	ks	175,00 Kč	175,00 Kč
XM-EZS-00230	Programování základních parametrů ústř.	16	hod	500,00 Kč	8 000,00 Kč
		0		0,00 Kč	0,00 Kč
XM-KAB-00020	Kabel do 10mm v trub.,liště	3830	m	12,00 Kč	45 960,00 Kč
XM-KAB-00290	Trubka PVC na om. vč. přích.	460	m	41,00 Kč	18 860,00 Kč
XM-KAB-00330	Elinstal. lišta do LV 40	118	m	41,00 Kč	4 838,00 Kč
XM-KAB-00910	Průchod zdívm do 100 cm D30	10	ks	204,00 Kč	2 040,00 Kč
	<b>Celkem</b>				<b>109 968,00 Kč</b>
<b>DPH:</b>	<b>DPH 21%</b>				<b>23 093,50 Kč</b>
	<b>Dodávky CCTV</b>				
Číslo položky	Popis položky	Počet	MJ	Jedn. cena	Celkem
IRH60L8A	IRH60L8A Světlo pro TD/N kamery, SMT LED, max. 40m(60°), 850	8	ks	4 990,00 Kč	39 920,00 Kč
SNC-EB632R	SNC-EB632R Venkovní IP bullet kamera, TD/N, HD 1080p, 2MP, M	7	ks	23 220,00 Kč	162 540,00 Kč
SNC-XM631	SNC-XM631 Vnitřní IP mini dome kamera, D/N, HD 1080p, 2MP, f	19	ks	9 450,00 Kč	179 550,00 Kč
HM507382R10040	HM507382R10040 NVR Husky M50 pro 40 IP kamer (zařízení), 16T	1	ks	337 340,00 Kč	337 340,00 Kč
WD40PURX	WD40PURX Přídavný HDD k rekordérům, 4TB	5	ks	5 290,00 Kč	26 450,00 Kč
	MS Win server	1	ks	12 000,00 Kč	12 000,00 Kč
		0		0,00 Kč	0,00 Kč
XPEBL	XPEBL; XProtect Enterprise 6.0 base licence	1	ks	55 370,30 Kč	55 370,30 Kč
XPECL	XPECL; XProtect Enterprise 6.0 camera licence	26	ks	5 616,00 Kč	146 016,00 Kč
MONH74A	MONH74A LCD TFT CCTV monitor 17", rozlišení 1280x1024, 5ms,	1	ks	4 700,00 Kč	4 700,00 Kč
	PC klient	1	ks	19 900,00 Kč	19 900,00 Kč
MONH245	MONH245 LCD TFT CCTV monitor 23.6" (16:9), rozlišení 1920x10	2	ks	8 700,00 Kč	17 400,00 Kč
	APC Smart-UPS RT 1000VA RM online	2	ks	18 500,00 Kč	37 000,00 Kč
	Průmyslový switch 2G-2S-1.4.1 BOX PoE+	11	ks	27 500,00 Kč	302 500,00 Kč
	miniGBIC SFP SC/WDM 100 Base	22	ks	682,70 Kč	15 019,40 Kč
P05D-SCSC-02	P05D-SCSC-02 Patch kabel KELine SC - SC Duplex 50/125 OM2 2	26	ks	138,32 Kč	3 596,32 Kč



KEL-C5E-T-015	KEL-C5E-T-015 Patch kabel KELine Giga 2xRJ45 Cat.5E S/FTP L	10	ks	21,06 Kč	210,60 Kč
383007225	VODIC SFTP CAT5E FRNC 4x2xAWG24	2170	m	14,18 Kč	30 770,60 Kč
2325/LPE-1	2325/LPE-1TRUBKA OHEBNA 320N	350	m	9,04 Kč	3 164,00 Kč
8,59506E+12	8595057610170 Lišta vkladací 40x 20 bílá LHD 2m	85	m	21,16 Kč	1 798,60 Kč
	<b>Celkem</b>				<b>1 395 245,82 Kč</b>
<b>DPH:</b>	<b>DPH 21%</b>				<b>293 001,50 Kč</b>
	<b>Montáže CCTV</b>				
Číslo položky	Popis položky	Počet	MJ	Jedn. cena	Celkem
XCTV-M000120	Montáž DOME kamery a zprovoznění	26	ks	525,00 Kč	13 650,00 Kč
XCTV-M000090	Uvedení do chodu a nast. kamery venkovní	26	ks	146,00 Kč	3 796,00 Kč
XCTV-M000170	Montáž venkovního IR reflektoru	8	ks	700,00 Kč	5 600,00 Kč
XCTV-M000200	Instalace záznamového zařízení	1	ks	2 500,00 Kč	2 500,00 Kč
XM-PC-00040	Zákl. parametrizace PC - TF	1	ks	3 100,00 Kč	3 100,00 Kč
XCTV-M000130	Montáž monitoru	3	ks	117,00 Kč	351,00 Kč
M-ZDR-00110	Instalace UPS	2	ks	350,00 Kč	700,00 Kč
XM-EZS-00230	Programování základních parametrů	20	hod	500,00 Kč	10 000,00 Kč
XCTV-M000230	Programování uživatelských požadavků	16	hod	500,00 Kč	8 000,00 Kč
XCTV-M000260	Instalace klientského SW na PC	10	hod	500,00 Kč	5 000,00 Kč
XM-STK-00240	Instalace akt. prvku bez managementu	11	ks	175,00 Kč	1 925,00 Kč
XM-STK-00140	Instalace Patch kabelu	36	ks	9,00 Kč	324,00 Kč
XM-KAB-00020	Kabel do 10mm v trub.,liště	2170	m	12,00 Kč	26 040,00 Kč
XM-KAB-00290	Trubka PVC na om. vč. přích.	350	m	41,00 Kč	14 350,00 Kč
XM-KAB-00330	Elinstal. lišta do LV 40	85	m	41,00 Kč	3 485,00 Kč
	<b>Celkem</b>				<b>98 821,00 Kč</b>
<b>DPH:</b>	<b>DPH 21%</b>				<b>20 752,50 Kč</b>
	<b>Dodávky LATIS</b>				
Číslo položky	Popis položky	Počet	MJ	Jedn. cena	Celkem
	PC server	1	ks	66 500,00 Kč	66 500,00 Kč
MONH74A	MONH74A LCD TFT CCTV monitor 17", rozlišení 1280x1024, 5ms,	1	ks	4 700,00 Kč	4 700,00 Kč
	MS Win server	1	ks	12 000,00 Kč	12 000,00 Kč
	PC klient	1	ks	21 500,00 Kč	21 500,00 Kč
MONH245	MONH245 LCD TFT CCTV monitor 23.6" (16:9), rozlišení 1920x10	2	ks	8 700,00 Kč	17 400,00 Kč
	APC Smart-UPS RT 1000VA RM online	1	ks	18 500,00 Kč	18 500,00 Kč
800038	SW LAT - administrační nástroj správy do 200 ADVANCED Admin	1	ks	20 000,00 Kč	20 000,00 Kč
800054	SW LOW- pracoviště výkonného operátora (pro system ADVANC	1	ks	8 000,00 Kč	8 000,00 Kč
800045	SW LGLE - editor grafických projektů LATIS Program, který vy	1	ks	29 900,00 Kč	29 900,00 Kč
800046	SW LDE - Latis data export Program pro export dat ze systému	1	ks	12 900,00 Kč	12 900,00 Kč

800039	SW - Latis COMINFO rozhraní LZEI Program pro připojení	1	ks	10 900,00 Kč	10 900,00 Kč
800052	SW LAOM - modul automatických činností Služba, pomocí které	1	ks	10 900,00 Kč	10 900,00 Kč
GXYSMART	GXYSMART Komunikační modul pro integraci ústředěn Galaxy do	1	ks	8 469,00 Kč	8 469,00 Kč
	<b>Celkem</b>				<b>241 669,00 Kč</b>
	<b>DPH: DPH 21%</b>				<b>50 750,50 Kč</b>
	<b>Montáže LATIS</b>				
Číslo položky	Popis položky	Počet	MJ	Jedn. cena	Celkem
XM-PC-00040	Zákl. parametrizace PC - TF	2	ks	3 100,00 Kč	6 200,00 Kč
XCTV-M000130	Montáž monitoru	3	ks	117,00 Kč	351,00 Kč
M-ZDR-00110	Instalace UPS	1	ks	350,00 Kč	350,00 Kč
XM-EZS-00230	Programování základních parametrů, instalace SW	20	hod	500,00 Kč	10 000,00 Kč
		0		0,00 Kč	0,00 Kč
XM-LAT-00292	Zadávání akt. prvku do grafické nadstavby a nastav. vazeb	1	kpl	48 500,00 Kč	48 500,00 Kč
800067	Vytvoření primárních mapových podkladů (půdorysů) - přehled	1	ks	1 500,00 Kč	1 500,00 Kč
800070	Vytvoření primárních mapových podkladů (půdorysů) - jedno	8	ks	3 500,00 Kč	28 000,00 Kč
	<b>Celkem</b>				<b>94 901,00 Kč</b>
	<b>DPH: DPH 21%</b>				<b>19 929,00 Kč</b>
	<b>Dodávky elektroinstalačního materiálu Hlavní trasa</b>				
Číslo položky	Popis položky	Počet	MJ	Jedn. cena	Celkem
RMA-37-L66-XAX-	19' rozvaděč stojanový 37U/600x600 dv. síť s 60% prostupnos	1	ks	8 648,75 Kč	8 648,75 Kč
RAC-CH-X02-A1	19' vent.j.-4V-220V/60W termostat RAL7035	1	ks	2 835,81 Kč	2 835,81 Kč
RAB-RP-X21-A1	19' rozvodný panel 6x220V-3m s vaničkou 1,5U RAL9005, dětská	1	ks	693,81 Kč	693,81 Kč
RAX-UP-450-A3	Polička perforovaná 1U/450mm, max.nosnost 80kg	2	ks	385,69 Kč	771,38 Kč
RAC-OJ-X01-A1	19' osvětlovací jednotka 1U RAL7035	1	ks	1 679,81 Kč	1 679,81 Kč
SHA-076062025-X	SHA-076062025-XCD Rozvaděč hybridní 760x620x250 mm na stěnu	3	ks	2 436,00 Kč	7 308,00 Kč
KAB-FO-X38-SL	KAB-FO-X38-SL Optická vana KELine neosazená pro 24 x SC Dup	5	ks	913,90 Kč	4 569,50 Kč
606029	606029 Patch panel KELine Giga 24xRJ45 Cat.5E STP černý 1U	5	ks	834,60 Kč	4 173,00 Kč
TB012M5	TB012M5 Optický kabel KELine univerzální 12-vláknový 50/125	420	m	31,20 Kč	13 104,00 Kč
2325/LPE-1	2325/LPE-1TRUBKA OHEBNA 320N	380	m	9,04 Kč	3 435,20 Kč
2153130	2153130 Příchytka MULTI-QUICK 25-28,5 2153130	380	ks	4,96 Kč	1 884,80 Kč
	<b>Celkem</b>				<b>49 104,06 Kč</b>
	<b>DPH: DPH 21%</b>				<b>10 312,00 Kč</b>

	<b>Montáže elektroinstalačního materiálu Hlavní trasa</b>				
Číslo položky	Popis položky	Počet	MJ	Jedn. cena	Celkem
XM-STK-00160	Montáž rozvaděče skříňového bez zapojení vodičů	1	ks	1 280,00 Kč	1 280,00 Kč
XM-STK-00180	Montáž ukládací police	2	ks	117,00 Kč	234,00 Kč
XM-STK-00190	Montáž napájecího panelu	1	ks	88,00 Kč	88,00 Kč
XM-STK-00210	Montáž ventilace	1	ks	175,00 Kč	175,00 Kč
XM-STK-00170	Montáž nástěnného rozvaděče bez zapojení vodičů	3	ks	1 280,00 Kč	3 840,00 Kč
XM-STK-00260	Montáž 19" FO rozvaděče do dat.rozv.	5	ks	350,00 Kč	1 750,00 Kč
XM-STK-00010	Montáž a zapojení Patch Panelu 24 portů	5	ks	1 800,00 Kč	9 000,00 Kč
XM-STK-00130	Instalace FO kabelu	420	m	18,00 Kč	7 560,00 Kč
XM-STK-00290	Zakončení optického kabelu - svár pig-tail	48	ks	250,00 Kč	12 000,00 Kč
XM-STK-00330	Měření a značení FO vlákna, měřicí protokol	48	ks	292,00 Kč	14 016,00 Kč
XM-KAB-00290	Trubka PVC na om. vč. přích.	380	m	41,00 Kč	15 580,00 Kč
	<b>Celkem</b>				<b>65 523,00 Kč</b>
<b>DPH:</b>	<b>DPH 21%</b>				<b>13 760,00 Kč</b>
	<b>Dodávky, Přístupové systémy výměna technologie</b>				
Číslo položky	Popis položky	Počet	MJ	Jedn. cena	Celkem
400637	V ASSET 808 X Řídící jednotka ASSET - 8 linek ( XPORT, FÓLIE	1	ks	34 500,00 Kč	34 500,00 Kč
400749	V ZDROJ PWR-532 V KRYTU Zálohovaný zdroj 5+3+2A kryt aku 60A	1	ks	6 200,00 Kč	6 200,00 Kč
PBQ12150	PBQ12150 Akumulátor 12V / 18Ah VdS	1	ks	1 404,00 Kč	1 404,00 Kč
400567	V ASSET 10 V KRYTU Dveřní modul - slouží k připojení čteček	42	ks	6 000,00 Kč	252 000,00 Kč
400609	V ASSET 20 V KRYTU Dveřní modul pro 2 čtečky pro 1 dveře- sl	1	ks	9 000,00 Kč	9 000,00 Kč
400565	V ASSET 602 RB čtečka TWM3	40	ks	5 500,00 Kč	220 000,00 Kč
400566	V ASSET 612 RB čtečka TWN3 s PIN	4	ks	6 500,00 Kč	26 000,00 Kč
400599	V ZDROJ PWR-3A/K40 Zálohovaný zdroj 3+2A v krytu pro aku 40A	5	ks	5 650,00 Kč	28 250,00 Kč
PBQ12150	PBQ12150 Akumulátor 12V / 18Ah VdS	5	ks	1 404,00 Kč	7 020,00 Kč
		0		0,00 Kč	0,00 Kč
400749	V ZDROJ PWR-532 V KRYTU Zálohovaný zdroj 5+3+2A kryt aku 60A	14	ks	6 200,00 Kč	86 800,00 Kč
PBQ12380	PBQ12380 Akumulátor 12V / 38Ah VdS	14	ks	3 007,00 Kč	42 098,00 Kč
		0		0,00 Kč	0,00 Kč
800008	SW ASSET server advanced Server. nadst. pro síť až 3 ústř. A	1	ks	30 500,00 Kč	30 500,00 Kč
800010	SW ASSET Klient SW pro klientskou stanicí ústředny Asset nut	1	ks	9 000,00 Kč	9 000,00 Kč

		0		0,00 Kč	0,00 Kč
383007225	VODIC SFTP CAT5E FRNC 4x2xAWG24	1880	m	14,18 Kč	26 658,40 Kč
	CYSY 2x1	975	m	9,50 Kč	9 262,50 Kč
2325/LPE-1	2325/LPE-1TRUBKA OHEBNA 320N	450	m	9,04 Kč	4 068,00 Kč
8,59506E+12	8595057610170 Lišta vkladací 40x 20 bílá LHD 2m	85	m	21,16 Kč	1 798,60 Kč
		0		0,00 Kč	0,00 Kč
400484	V LML-8 LINKOVÝ MODUL Linkový modul pro systémy ASSET v kryt	1	ks	2 820,00 Kč	2 820,00 Kč
400581	V KLÁVESNICE KMU-4 Klávesnice pro ovládání ústředn ASSET, M	1	ks	3 100,00 Kč	3 100,00 Kč
	<b>Celkem</b>				<b>800 479,50 Kč</b>
<b>DPH:</b>	<b>DPH 21%</b>				<b>168 100,50 Kč</b>
	<b>Montáže, Přístupové systémy výměna technologie</b>				
Číslo položky	Popis položky	Počet	MJ	Jedn. cena	Celkem
XM-EZS-00010	Montáž ústředny	1	ks	1 400,00 Kč	1 400,00 Kč
XM-EZS-00230	Programování základních parametrů ústř.	24	hod	500,00 Kč	12 000,00 Kč
XM-ZDR-00010	Montáž zdroje s dobíječem v OC skříni	20	ks	525,00 Kč	10 500,00 Kč
XM-ZDR-00040	Instalace akumulátoru	20	ks	117,00 Kč	2 340,00 Kč
XACS-M00070	Montáž rozvodného členu	43	ks	350,00 Kč	15 050,00 Kč
XACS-M00080	Montáž čtečky	44	ks	250,00 Kč	11 000,00 Kč
XM-KAB-00020	Kabel do 10mm v trub.,liště	2855	m	12,00 Kč	34 260,00 Kč
XM-KAB-00290	Trubka PVC na om. vč. přích.	450	m	41,00 Kč	18 450,00 Kč
XM-KAB-00330	Elinstal. lišta do LV 40	85	m	41,00 Kč	3 485,00 Kč
XM-EZS-00050	Montáž expanderu	1	ks	700,00 Kč	700,00 Kč
XM-EZS-00020	Montáž klávesnice	1	ks	350,00 Kč	350,00 Kč
	<b>Celkem</b>				<b>109 535,00 Kč</b>
<b>DPH:</b>	<b>DPH 21%</b>				<b>23 002,50 Kč</b>
	<b>Ostatní</b>				
Číslo položky	Popis položky	Počet	MJ	Jedn. cena	Celkem
XM-VRN-0040	Dokumentace skutečného provedení	1	kpl	98 000,00 Kč	98 000,00 Kč
XM-VRN-0130	Funkční zkouška	1	kpl	16 200,00 Kč	16 200,00 Kč
XM-VRN-0140	Výchozí revize	1	kpl	18 200,00 Kč	18 200,00 Kč
XM-VRN-0190	Drobný instalační materiál	1	kpl	22 500,00 Kč	22 500,00 Kč
XM-VRN-0090	Doprava osobní	1	kpl	81 000,00 Kč	81 000,00 Kč
	Koordinační práce	1	kpl	12 650,00 Kč	12 650,00 Kč
	<b>Celkem</b>				<b>248 550,00 Kč</b>
<b>DPH:</b>	<b>DPH 21%</b>				<b>52 195,50 Kč</b>

Příloha 2	Výkres č. 01 – Doplnění zabezpečení U5 - 1.NP (CD)
Příloha 3	Výkres č. 02 - Doplnění zabezpečení U5 - 2.NP (CD)
Příloha 4	Výkres č. 03 – Doplnění zabezpečení U5 – 3.NP (CD)
Příloha 5	Výkres č. 04 – Doplnění zabezpečení U5 – 4.NP (CD)
Příloha 6	Výkres č. 05 – Doplnění zabezpečení U5 – 5.NP (CD)
Příloha 7	Výkres č. 06 – Doplnění zabezpečení U5 – 6.NP (CD)
Příloha 8	Výkres č. 07 – Doplnění zabezpečení U5 – 7.NP (CD)