

Návrh zabezpečení datového centra a zajištění zálohování dat pomocí datového úložiště na síti

A Design for the Protection of Data Centers and Ensuring Data Backup Using NAS Technology

Bc. Lukáš Králík

Diplomová práce
2012



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Lukáš KRÁLÍK**
Osobní číslo: **A10322**
Studijní program: **N 3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**

Téma práce: **Návrh zabezpečení datového centra a zajištění zálohování dat pomocí datového úložiště na síti**

Zásady pro vypracování:

1. Provedte průzkum trhu s ohledem na zabezpečovací prvky.
2. Navrhněte zabezpečení datového centra (přístupový a dohledový systém, požární ochrana, ...).
3. Analyzujte možnosti pro zálohování důležitých dat.
4. Popište technologii NAS.
5. Navrhněte řešení automatických záloh pomocí NAS.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 3. aktualiz. S.l. : Cricetus, 2006. 313 s. ISBN 80-902938-2-4.**
2. **KINDL, Jiří. Projektování bezpečnostních systémů I. 2. vyd. Zlín : Univerzita Tomáše Bati, 2007. 134 s. ISBN 978-80-7318-554-1.**
3. **BEBČÁK, Petr. Požárně bezpečnostní zařízení. 2. vyd. V Ostravě : Sdružení požárního a bezpečnostního inženýrství, 2004. 130 s. ISBN 80-86634-34-5.**
4. **XIAO, Yang; LI, Frank Haizhon; CHEN, Hui. Handbook of security and networks. New Jersey : World Scientific, 2011. 551 s. ISBN 978-981-4273-03-9.**
5. **JAŠEK, Roman. Ochrana znalostí a dat v podnikových informačních systémech. Vyd. 1. Zlín: Univerzita Tomáše Bati, Fakulta managementu a ekonomiky, 2002, 115 s. ISBN 80-731-8095-2.**
6. **JAŠEK, Roman. Informační a datová bezpečnost. Zlín : Univerzita Tomáše Bati ve Zlíně, Fakulta managementu a ekonomiky, 2006. 140 s. ISBN 80-7318-456-7.**

Vedoucí diplomové práce:

Ing. Jiří Korbek, Ph.D.

Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce:

24. února 2012

Termín odevzdání diplomové práce:

15. května 2012

Ve Zlíně dne 24. února 2012



prof. Ing. Vladimír Vašek, CSc.
děkan



doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Práce ve stručnosti shrnuje problematiku zabezpečení a provozu datového centra a zaměřuje se především na fyzickou stránku této problematiky. Jsou zde obsaženy úplné základy ohledně bezpečnostních systémů, tak i základy datového centra, případně zálohování a jejich vzájemné propojení s využitím možností technologie datového úložiště na síti, neboli NAS.

Klíčová slova: datové centrum, NAS, datové úložiště na síti, zálohování, bezpečnostní systémy, návrh zabezpečení.

ABSTRACT

This work briefly summarizes the problems around protection and service of data center. It's specifically focuses on physical protection. There can be found a basic knowledge about security systems or about whole data center and ensuring data backup using NAS technology.

Keywords: data center, NAS, network attached storage, backup, security systems, design for the protection.

Na tomto místě bych rád poděkoval řadě lidí, bez jejichž pomoci, cenných rad a zkušeností by tato práce nevznikla. V první řadě je to pan Ing. Jiří Korbel Ph.D., pod jehož odborným dohledem a vedením tato práce vznikla. Mé poděkování též patří panu Ing. Janu Valouchovi Ph.D., za jeho zkušenosti a postřehy, které byly neocenitelné a byly mi přínosem při návrhu poplachového systému. Dále je to pan Ing. Petr Kováč, bez jehož pomoci a ochoty by nemohla tato práce být doplněna o výkresy. A v neposlední řadě bych chtěl poděkovat své manželce a rodině, která mě byla nejen po dobu psaní práce, ale po celou dobu studia velkou oporou.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně

.....
podpis diplomanta

OBSAH

ÚVOD	11
I TEORETICKÁ ČÁST	12
1 DATOVÉ CENTRUM	13
1.1 ÚROVNĚ DATOVÉHO CENTRA.....	13
1.1.1 Fault tolerant infrastruktura.....	14
1.2 STRUKTURA DATOVÉHO CENTRA	14
1.2.1 MDA – Main distribution area.....	14
1.2.2 HDA – Horizontal Distribution Area.....	14
1.2.3 ZDA – Zone Distribution Area.....	15
1.2.4 EDA – Equipment Distribution Area.....	15
1.3 ÚLOŽIŠTĚ DAT.....	16
1.3.1 Diskové pole.....	16
1.3.2 DAS	16
1.3.3 SAN	17
1.3.4 NAS	18
1.4 BEZPEČNOST DATOVÉHO CENTRA	19
1.4.1 Fyzická bezpečnost	20
2 MECHANICKÉ ZÁBRANNÉ SYSTÉMY	22
2.1 PRŮLOMOVÁ ODOLNOST.....	22
2.2 MECHANICKÉ ZÁBRANNÉ SYSTÉMY PLÁŠŤOVÉ OCHRANY	24
2.2.1 Stavební otvory.....	24
2.3 PŘEDMĚTOVÁ OCHRANA	24
2.4 APLIKACE MZS PRO DATOVÁ CENTRA A INFORMAČNÍ TECHNOLOGIE.....	25
2.4.1 Datové sejfy.....	25
2.4.2 Média sejfy	26
2.4.3 Zabezpečený rack.....	26
2.4.4 Datové komory	27
3 POPLACHOVÉ ZABEZPEČOVACÍ A TÍŠŇOVÉ SYSTÉMY	29
3.1 STUPEŇ ZABEZPEČENÍ.....	30
3.2 TŘÍDA PROSTŘEDÍ	31
3.3 OSTATNÍ VLIVY	32
3.3.1 Vlivy působící vně chráněného objektu.....	32
3.3.2 Vlivy působící uvnitř chráněného objektu	32
3.4 OBVODOVÁ OCHRANA.....	33
3.5 PLÁŠŤOVÁ OCHRANA	33
3.5.1 Magnetické kontakty.....	33
3.5.2 Detektory rozbití skla.....	34

3.6	PROSTOROVÁ OCHRANA.....	34
3.6.1	Pasivní infračervené detektory.....	35
3.6.2	Mikrovlnné detektory.....	37
3.6.3	Ultrazvukové detektory.....	38
3.6.4	Duální detektory	38
3.7	ÚSTŘEDNY PZTS	38
3.7.1	Drátové ústředny	39
3.7.1.1	Smyčková.....	40
3.7.1.2	Sběrníková ústředna.....	40
3.7.1.3	Smíšená ústředna	40
3.7.2	Bezdrátové ústředny	41
3.7.3	Hybridní ústředny.....	41
4	SYSTÉMY KONTROLY VSTUPU	42
4.1	PŘÍSTUPOVÉ SYSTÉMY	43
4.1.1	Autonomní.....	43
4.1.2	Skupinové.....	44
4.1.3	Globální - síťové	44
4.2	ELEKTRONICKÉ PRVKY	44
4.2.1	Čip.....	44
4.2.2	Čtečky	45
4.2.3	Řídicí jednotka.....	46
4.2.4	Napájecí zdroj.....	46
4.2.5	Kabelové rozvod.....	46
4.3	ELEKTRICKY OVLÁDANÉ PRVKY	47
5	PROTIPOŽÁRNÍ OCHRANA	48
5.1	ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE	48
5.1.1	Základní rozdělení EPS	48
5.2	SOUČÁSTI SYSTÉMU EPS.....	49
5.2.1	Ústředna EPS	49
5.2.2	Hlásiče požáru	50
5.2.2.1	Tlačítkové hlásiče	50
5.2.2.2	Samočinné hlásiče.....	50
5.2.2.3	Ionizační hlásič kouře.....	51
5.2.2.4	Optický hlásič kouře	52
5.2.2.5	Hlásiče teplot.....	53
5.3	STABILNÍ HASICÍ ZAŘÍZENÍ.....	53
5.3.1	Plynová SHZ.....	54
6	ZDROJE NEPŘERUŠOVANÉHO NAPÁJENÍ	55
6.1	TYPY UPS	56
6.1.1	Off-line	56
6.1.2	Line-interactive.....	57
6.1.3	On-line.....	57

6.2	SYSTEMY UPS	58
6.2.1	Paralelní.....	59
6.2.2	Redundantní.....	59
6.3	KOMUNIKAČNÍ ROZHRANÍ	59
7	KLIMATIZACE A VZDUCHOTECHNIKA	60
7.1	KOMFORTNÍ KLIMATIZACE.....	60
7.1.1	Split systém.....	60
7.2	PŘESNÁ KLIMATIZACE	61
7.2.1	Freecooling	62
7.3	NÁVRH KLIMATIZACE DATOVÝCH CENTER	63
7.3.1	Návrh chlazení malých datových center	63
7.3.1.1	Požadavky na klimatizační zařízení.....	65
7.3.1.2	Určení chladicího výkonu	65
7.3.2	Návrh chlazení středních a velkých datových center.....	65
8	ZÁLOHOVÁNÍ.....	68
8.1	NEJČASTĚJŠÍ PŘÍČINY ZTRÁTY DAT.....	68
8.1.1	Lidský faktor	68
8.1.2	Selhání operačního systému.....	69
8.1.3	Chyba aplikace.....	69
8.1.4	Viry	69
8.1.5	Hardwarová porucha.....	69
8.1.6	Živelné pohromy	70
8.2	METODY ZÁLOHOVÁNÍ	70
8.2.1	Ruční zálohování dat.....	70
8.2.2	Automatizované ruční zálohování dat	70
8.2.3	Kopírování dat s komprimací.....	71
8.2.4	Automatizované zálohování dat s komprimací	71
8.2.5	Vytváření obrazu.....	71
8.3	TYPY ZÁLOH	72
8.3.1	Nestrukturovaná	72
8.3.2	Úplná + Inkrementální.....	72
8.3.3	Úplná + Rozdílová	72
8.3.4	Zrcadlová + Reverzně přírůstková.....	72
8.3.5	Úplná záloha systému.....	73
8.4	ZÁLOHOVACÍ MÉDIA	73
8.4.1	DVD disky.....	73
8.4.2	Pevné disky.....	73
8.4.3	Flash paměti.....	73
8.4.4	NAS	74
8.4.5	Online zálohování.....	74
II	PRAKTICKÁ ČÁST.....	75
9	NÁVRH ŘEŠENÍ AUTOMATICKÝCH ZÁLOH POMOCÍ TECHNOLOGIE NAS.....	76

9.1	DÁVKOVÝ SOUBOR A PLÁNOVAČ ÚLOH.....	76
9.1.1	Vytvoření dávkového souboru	76
9.1.2	Vytvoření naplánované úlohy	77
9.2	FUJITSU NETBAK REPLICATOR	78
9.3	COBIAN BACKUP	83
10	NÁVRH ZABEZPEČENÍ DATOVÉHO CENTRA.....	88
10.1	ÚDAJE O KLIENTOVI	88
10.2	ÚDAJE O STŘEŽENÝCH OBJEKTECH.....	88
10.2.1	Základní údaje.....	88
10.2.2	Půdorys objektu	90
10.2.3	Rozpis místností a třída prostředí	92
10.3	STUPEŇ ZABEZPEČENÍ.....	94
10.4	PŘEHLED ZAŘÍZENÍ.....	94
10.5	KONFIGURACE SYSTÉMU	97
10.5.1	Rozdělení do zón	98
10.5.2	Rozmístění prvků	99
10.6	HLÁŠENÍ POPLACHU	101
10.7	NORMY A LEGISLATIVA	101
10.8	CERTIFIKÁTY	101
10.9	ZÁSAH	101
10.10	ÚDRŽBA A OPRAVY	102
	ZÁVĚR	103
	CONCLUSION.....	104
	SEZNAM POUŽITÉ LITERATURY	105
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	108
	SEZNAM OBRÁZKŮ	111
	SEZNAM TABULEK	113
	SEZNAM PŘÍLOH	114
	PŘÍLOHA P I: ROZPOČET	115
	PŘÍLOHA P II: NÁVRH DALŠÍCH OPATŘENÍ.....	116
	PŘÍLOHA P III: POUŽITÉ SCHEMATICKE ZNAČKY.....	119
	PŘÍLOHA P IV: CERTIFIKÁTY PRVKŮ SYSTÉMU.....	120
	PŘÍLOHA P V: OBSAH DISKU CD	122

ÚVOD

V souvislosti s prudkým rozvojem informačních a komunikačních technologií, zejména pak jejich vzájemného propojení, naše společnost získává naprosto nový rozměr a můžeme tak mluvit o informační společnosti. Právě díky informační společnosti se ocitáme na prahu zcela nových základů a principů svého fungování. Běžně používáme pojmy jako je kyberprostor či virtuální svět. Přitom do nedávna jsme se s těmito pojmy setkávali pouze ve vědeckofantastické literatuře nebo filmech.

Díky tomuto rozvoji si dnes jistě celá řada firem nedokáže představit svou existenci bez internetu, nebo vůbec bez počítačů. Vznikají firemní sítě, jejichž srdcem i mozkiem jsou datová centra. Místa kde firmy uchovávají většinou své nejcennější informace, své know-how a nejen to. Dříve byly datová centra dominantou převážně obrovských nadnárodních společností, to proto, že ostatní firmy si je z finančních důvodů nemohli dovolit. Současná situace je však naprosto odlišná. Své malé datové centrum, si dnes může díky technickému pokroku dovolit téměř každý. Ovšem nese to s sebou i řadu problémů a úskalí. Jedním z řady problémů a snad i nejzávažnější je bezpečnost.

Samozřejmě, že na bezpečnost můžeme nahlížet z mnoha různých úhlů pohledu. Datová bezpečnost, personální bezpečnost, a tak dále. Tato práce se zaměřuje na fyzickou bezpečnost, ovšem je nutné podotknout, že jednotlivé úhly pohledu se vzájemně prolínají a názory na daný problém jsou velice individuální. Někdo za určitým opatřením může vidět právě personální bezpečnost, jiný naopak datovou.

I. TEORETICKÁ ČÁST

1 DATOVÉ CENTRUM

Pod pojmem datové centrum si můžeme představit specializované prostory určené k umístění informačních a komunikačních technologií. Úkolem datového centra je těmto technologiím zajistit stabilní a bezpečné prostředí pro jejich nepřetržitý provoz bez vlivů okolního prostředí. Datové centrum lze definovat jako souhrn technických prostředků potřebných k provozování informačních systémů.

Koncepce datového centra není nijak striktně definována a je ovlivňována především vývojem jednotlivých technologií. Nicméně existuje norma, která stanovuje podmínky a prostředí ve kterém jsou technologie provozovány. Normu pod označením TIA – 942: Data Center Standard vymezuje umístění technologií, napájení, uspořádání kabeláže, ale také zabezpečení. Čím se norma nezabývá, je design datového centra.[1]

Datová centra lze rozdělit podle mnoha hledisek, podle velikosti (malá, střední, velká), podle účelu (kolokační – pronájem místa jiným podnikům, podniková – pro vlastní účely podniku), nebo podle normy, která je rozděluje podle dostupnosti do čtyř úrovní – tier level.

1.1 Úrovně datového centra

1) Tier level 1

- Jednoduché (non-redundant – bez nadbytečného) připojení a propojení.
- Non-redundant výpočetní prostředky a technologie.
- Dostupnost 99,671% (maximální doba výpadku < 29 hodin/rok).

2) Tier level 2

- Redundantní výpočetní prostředky a technologie.
- Dostupnost 99,741% (maximální doba výpadku < 23 hodin/rok).

3) Tier level 3

- Duální napájení provozovaných komponent.
- Redundantní připojení i propojení provozovaných komponent.
- Vzájemná kompatibilita nasazených komponent.
- Možnost údržby systémů bez omezení/přerušení provozu.
- Dostupnost 99,982% (maximální doba výpadku < 90 minut/rok).

4) Tier level 4

- Veškeré technologické prostředky podílející se na provozu musí být zálohované nezávislým napájením (klimatizace, ventilace, topení, ...).
- Duální napájení provozovaných komponent.
- Redundantní připojení i propojení provozovaných komponent.
- Fault tolerant infrastruktura.
- Možnost údržby systémů bez omezení/přerušení provozu.
- Dostupnost 99,995% (maximální doba výpadku < 45 minut/rok).[2]

1.1.1 Fault tolerant infrastruktura

Jedná se o technologii, která umožňuje provoz i v případě, kdy vypadne jedna, nebo více komponent systému. Jako příklad lze použít úložiště dat – pro případ, že vypadne některý z pevných disků, se využívá RAID technologie. K dalším používaným technologiím patří replikace nebo clustering.

1.2 Struktura datového centra

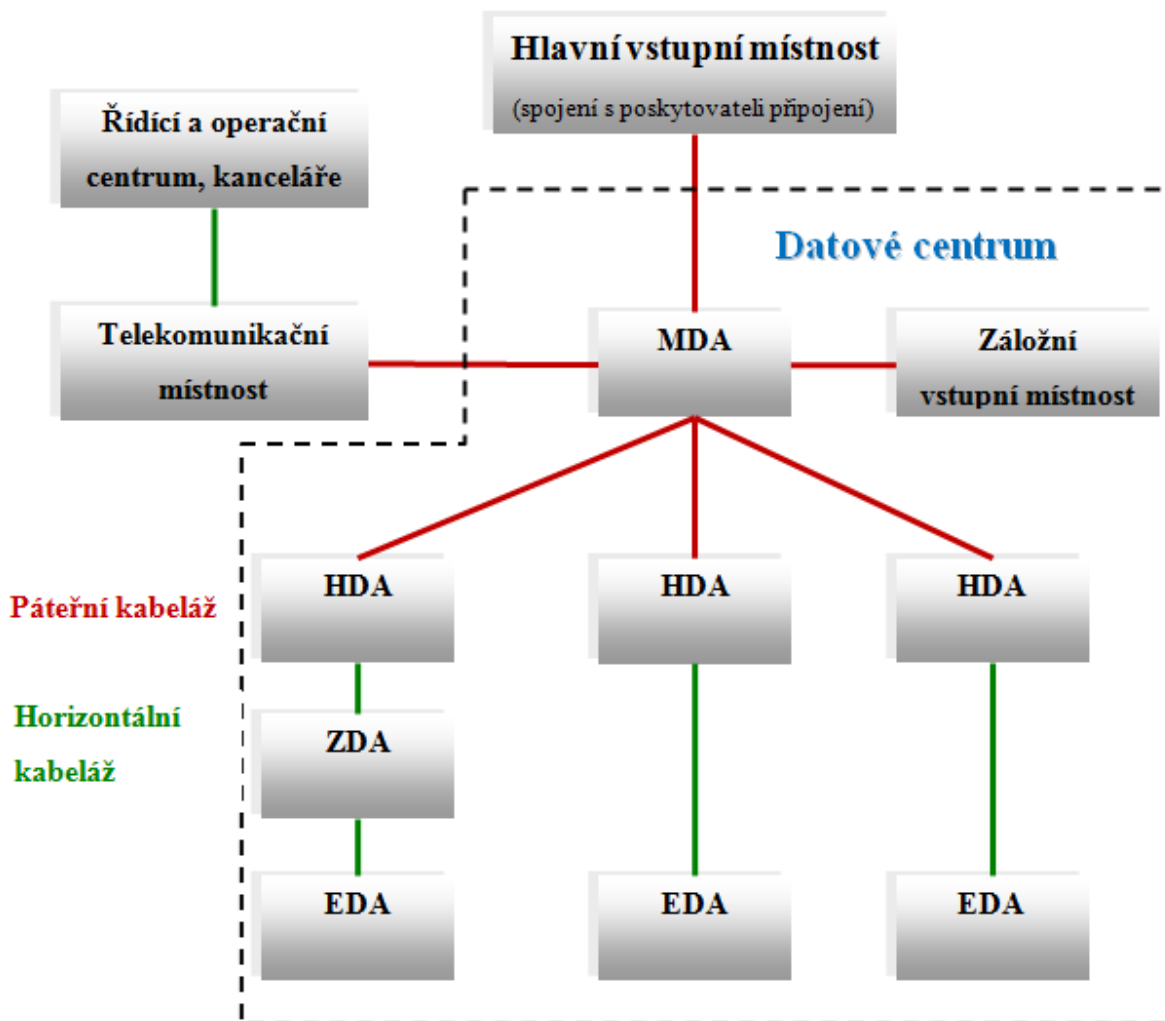
Jak již bylo řečeno, mezinárodní norma TIA – 942 standardizuje koncept, nebo chceme-li konstrukci, strukturu datového centra (obr. 1). [2]

1.2.1 MDA – Main distribution area

Je udávána jako centrální místo pro připojení datových center. Tento uzel je určen pro umístění centrálních prvků a je zde umístěný. Zajišťuje také spojení s WAN (Wide Area Network) a s poskytovateli telekomunikačních služeb přes vstupní místnost.[1]

1.2.2 HDA – Horizontal Distribution Area

Distribuční bod kabeláže pro přístrojovou oblast. Je připojen k hlavnímu rozvaděči pomocí výkonných datových kabelů a pomocí optických kabelů. Jednotlivé uzly HDA jsou umístovány v samotných centrech připojení, popřípadě jsou umístovány do prvních rozvaděčů EDA nebo přímo do EDA. Jde především o LAN (Local Area Network) a SAN (Storage Area Network), switche, ...[1]



Obrázek 1: Struktura datového centra [2]

1.2.3 ZDA – Zone Distribution Area

Bod spojující mezi sebou HDA a EDA. Tento bod se využívá převážně k realizaci velkých datových center, která využívají rozdělení do tzv. uliček. Díky tomu není nutné vedení kabelů z každého serveru do HDA, servery a jiná síťová zařízení jsou nejprve připojeny do ZDA, odkud se dál vedou společně do HDA.[1]

1.2.4 EDA – Equipment Distribution Area

V EDA rozvaděčích jsou umístěna hostitelská zařízení jako jsou servery, disková pole, síťové zdroje a konektivita do HDA. V malých datových centrech jsou většinou přímo propojeny do HDA.[1]

1.3 Úložiště dat

Technologií pro ukládání dat je poměrně mnoho - od lokálních datových úložišť připojených přímo k jednotlivým serverům, přes centrální disková úložiště až po diskové systémy připojené přímo do místní sítě, přes kterou jsou přístupné jak serverům, tak uživatelům. V současnosti se využívají tyto technologie ukládání dat:

- 1) diskové pole
- 2) DAS (Directly Attached Storage)
- 3) SAN (Storage Area Network)
- 4) NAS (Network Attached Storage)

1.3.1 Diskové pole

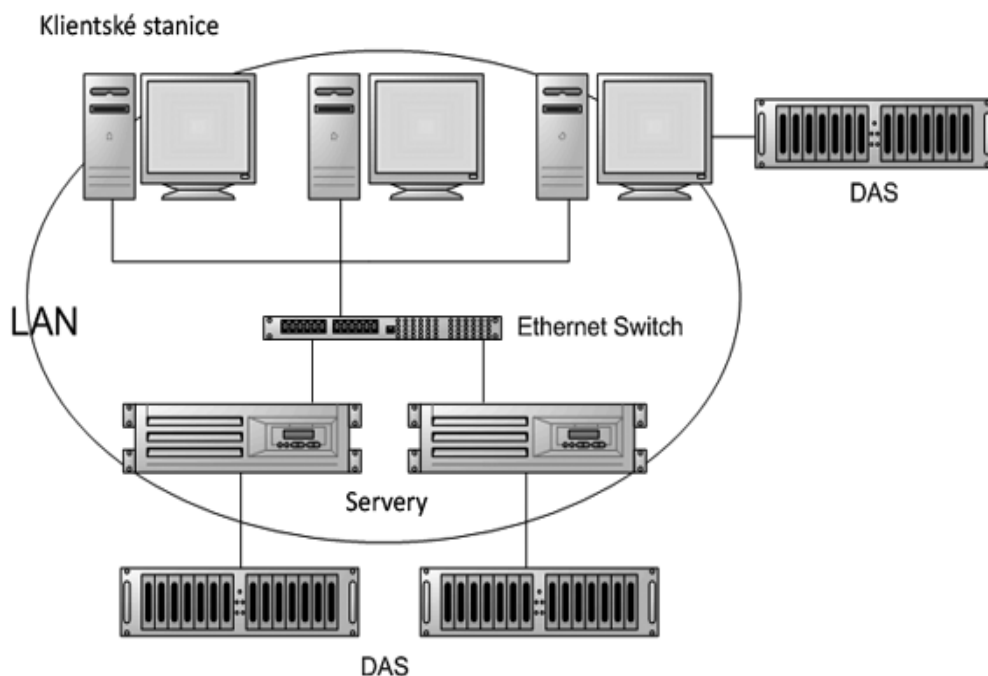
Diskovým polem rozumíme externí zařízení s jedním nebo více (z důvodu redundance) diskovými řadiči (controllery), které komunikují se servery na blokové úrovni. Základem této komunikace je sada SCSI příkazů a transportní vrstva. Tou může být:

- 1) SCSI = nejstarší, v současné době je nahrazována modernějšími a výkonnějšími technologiemi
- 2) FC = FibreChannel, nejprofesionálnější a nejčastěji nasazované řešení, zpravidla na optických linkách. Aktuálně s rychlostí až 8Gbit/s
- 3) SAS = Serial attached SCSI, jedná se o sériovou podobu SCSI, v současné době s rychlostí až 6Gbit/s
- 4) iSCSI - v počátcích vyvíjeno jako levnější alternativa k FC infrastruktuře, sériová podoba SCSI přes transportní vrstvu LAN. Nyní již plně výkonově srovnatelná technologie s FC. V současné době nabízí rychlost až 10Gbit/s. [3]

1.3.2 DAS

Je úložiště přímo připojené k serveru. Tento na první pohled nejlogičtější způsob má však řadu nevýhod. Při poruše serveru jsou data nepřístupná. V některém serveru může být velké množství volného místa, u jiného může docházet k nedostatku volného místa. Také možnosti rozšíření diskové kapacity nebo správa jsou značně omezené. Dalším problémem je vzdálenost samotného serveru a úložiště, buď jsou disky instalovány přímo v serveru,

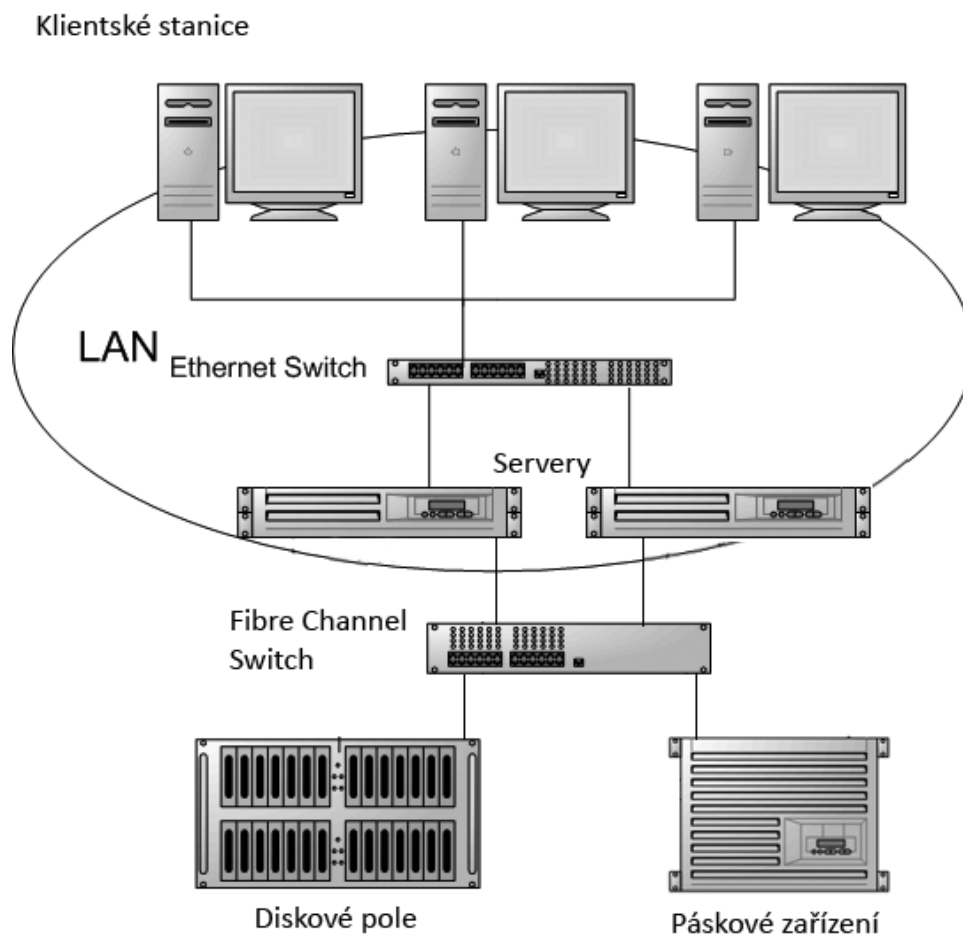
nebo externím diskovém poli, každopádně délky připojovacích kabelů (běžně SCSI) představují limitující faktor.



Obrázek 2: Schéma technologie DAS

1.3.3 SAN

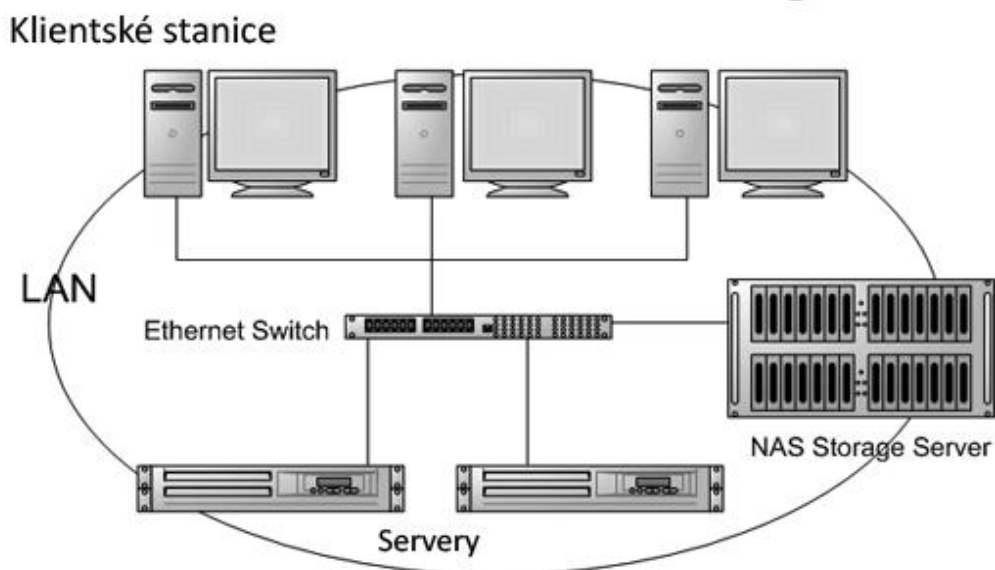
Je síť sdílených datových úložišť, jako jsou disková pole nebo pásková zařízení. Architektura SAN je taková, že datová úložiště jsou k dispozici pro více serverů, ať už v místní síti LAN (Local Area Network), tak i v síti WAN (Wide Area Network). Vzhledem k tomu, že uložená data nejsou umístěny přímo na některém serveru, je tak možné využít výpočetního výkonu serverů k optimalizaci podnikových aplikací. Výhodou je také využití volného místa datového úložiště na tom serveru, na kterém je právě potřeba. Jedná se vlastně o sdílenou kapacitu datového úložiště.



Obrázek 3: Schéma technologie SAN [4]

1.3.4 NAS

Datové úložiště se fyzicky skládá ze sady pevných disků (SAS, SATA), řadiče diskového pole RAID, síťové karty, procesoru a příslušného softwarového vybavení pro řízení, konfiguraci a mapování souborového systému. Základní modely představují zařízení v provedení Tower nebo 1U rack, s kapacitami od 1TB, špičkové modely dosahují kapacity až desítek PB (petabyte). Zařízení umožňují použít redundantní síťové karty, či napájecí zdroje. Disky jsou typu Hot-Plug, tedy vyměnitelné za plného provozu, což zajišťuje vysokou dostupnost celého systému.[3]



Obrázek 4: Schéma technologie NAS

NAS umožňuje variabilitu jak do počtu, tak i kapacity pevných disků, variabilitu jejich přiřazení jednotlivým serverům. Odpadá zde také nutnost restartování operačního systému serveru v případě doplnění disků. Umístění NAS zařízení je možné kdekoliv v rámci místní sítě LAN. Samozřejmostí je podpora různých platform OS (operační systém) a najednou mohou být obslouženy různé typy operačních systémů, servery nebo klientské stanice. [4]

1.4 Bezpečnost datového centra

Při provozu datového centra je nutné věnovat značnou pozornost bezpečnosti. Jak bylo zmiňováno výše, bezpečnost datového centra řeší i mezinárodní norma TIA-942. Ta však nezabíhá do detailů a stanovuje pouze protipožární ochranu, případnou ochranu před vniknutím vody, pokud toto riziko hrozí, a doporučuje kontrolu přístupu do vstupní místnosti. V neposlední řadě se zabývá operačními parametry:

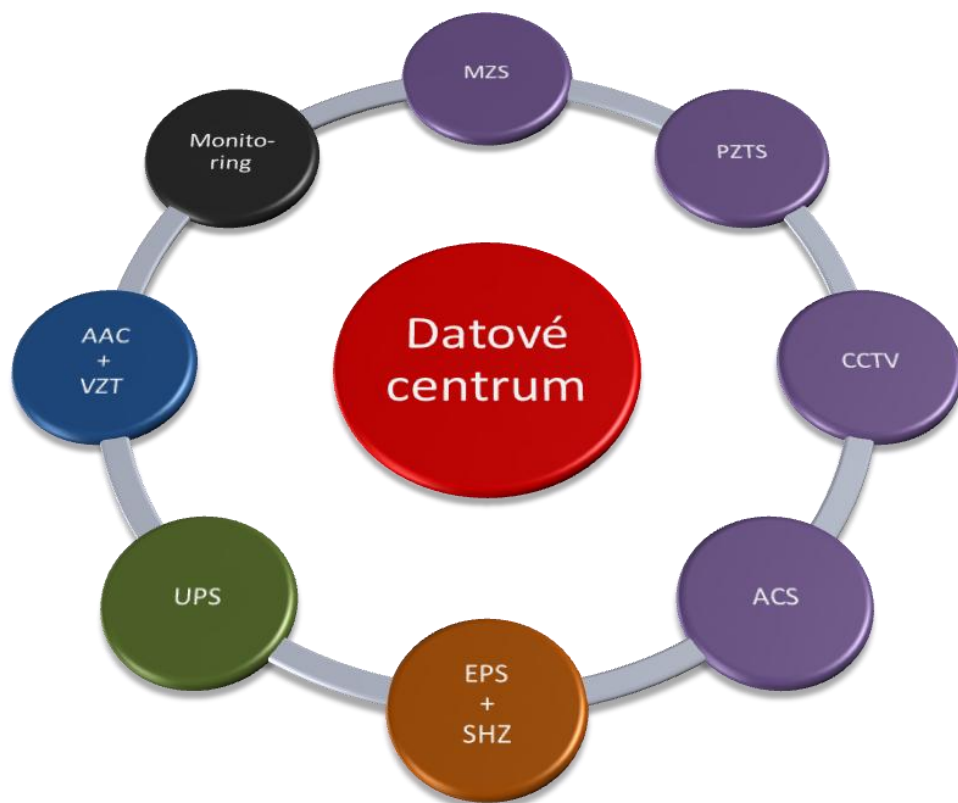
- 1) Teplota suchého teploměru: 20 °C – 25 °C.
- 2) Relativní vlhkost: 40% – 55%.
- 3) Maximální rosný bod: 21 °C.
- 4) Maximální rychlost změny teploty: 5 °C za hodinu.[2]

Čím se norma nezabývá, je fyzická a datová bezpečnost, je tedy čistě na provozovateli datového centra, zda bude investovat prostředky do těchto zabezpečení.

Datovou bezpečností je většinou myšleno především zálohování dat, pokud tedy datové centrum nezpracovává osobní údaje, nebo dokonce utajované informace. Nejčastěji se však datová centra zabezpečují hlavně fyzicky.

1.4.1 Fyzická bezpečnost

Fyzická bezpečnost neodmyslitelně patří k ochraně datových center, nebo přesněji řečeno dat vůbec. Co si pod pojmem fyzická bezpečnost představit? Jde o soubor technických prostředků a režimových opatření použitých k zajištění bezproblémovému bezpečnému chodu datového centra. Tyto technické prostředky si můžeme představit jako takový hardware, který dále můžeme rozdělit podle funkce, kterou v systému zastává.



Obrázek 5: Schéma fyzické bezpečnosti datového centra

- 1) **Řízení přístupu a ochrana proti neoprávněnému vniknutí**
 - Mechanické zábranné systémy (MZS)
 - poplachové zabezpečovací a tísňové systémy (PZTS)
 - systém kontroly vstupu (ACS)
 - kamerový systém (CCTV)

2) Protipožární ochrana a zhasací systém

- elektronická požární signalizace (EPS)
- instalace stabilního hasicího zařízení (SHZ)

3) Záložní napájení

- Identifikace kritických aplikací
- Záložní napájecí zdroje (UPS)

4) Klimatizace a vzduchotechnika (AAC a VZT)**5) Monitoring**

- lokální monitoring vybraných kritických aplikací a prvků datového centra
- vzdálený monitoring datového centra

2 MECHANICKÉ ZÁBRANNÉ SYSTÉMY

O mechanických zábranných systémech můžeme mluvit jako o elementárním prvku fyzické ochrany. Jejich primárním úkolem je odradit případného pachatele a znemožnit mu tak vniknout do střeženého objektu, nebo alespoň mu jeho počínání co nejvíce zkomplikovat. Nicméně mechanické zábranné systémy lze ve fyzické ochraně datových center využít i jinak než jen k zamezení přístupu neoprávněné osoby například k serveru. Důležitou roli hrají i při ochraně vybavení datových center, respektive vůbec IT zařízení nebo informací před poškozením následky požáru. Jsou to tedy jejich mechanické vlastnosti, nebo dalo by se říct, že se jedná o odpor proti působení vnějších vlivů destruktivní povahy. V této souvislosti se tedy bavíme o průlomové odolnosti.

2.1 Průlomová odolnost

Každé zabezpečení je překonatelné, a to v závislosti od množství potřebné energie vynaložené k překonání překážky, času, fyzických dispozic (zručnosti) narušitele a typu použitého nářadí. Prvky mají své základní vlastnosti například fyzikální, mechanické a izolační. S ohledem na průlomovou odolnost nás zajímají především ty mechanické vlastnosti jako je pevnost, tvrdost a další.[5]

Stanovení minimální doby průlomové odolnosti (MDPO)

$$t_{VLOUPÁNÍ} = t_2 - t_1 \text{ [min]}$$

$t_{VLOUPÁNÍ}$ časový interval potřebný k překonání překážky

t_2 čas konečného překonání překážky

t_1 čas začátku útoku na překážku

Stanovení MDPO úschovných objektů

$$t_{VLOUPÁNÍ} = [(V_R - B_V) : C_1] \cdot f \text{ [min]}$$

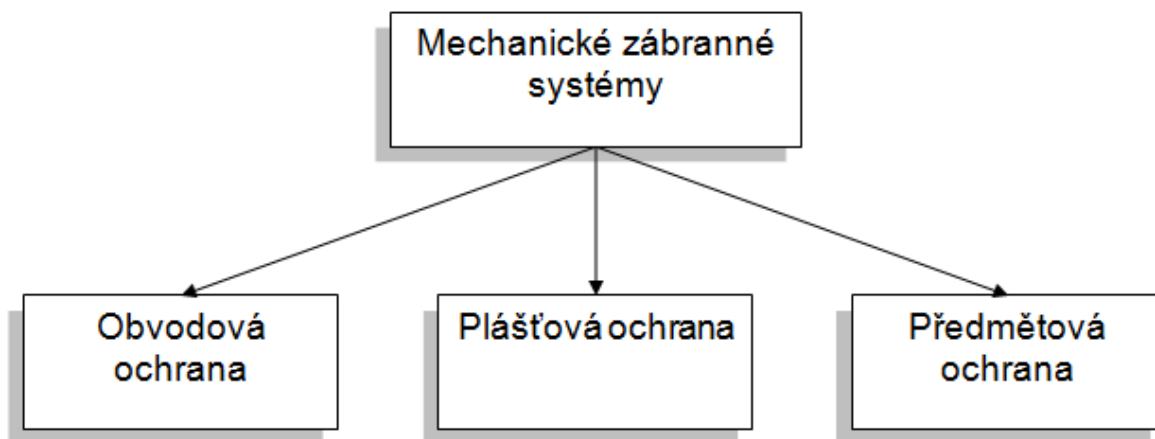
V_R hodnota průlomové odolnosti úschovného objektu

B_V základní ocenění, číselná hodnota přiřazená určitému nářadí

C_1 koeficient průlomové odolnosti úschovného objektu.

f koeficient navýšení (2-3)

MZS je možné rozdělit do tří základních skupin a to podle jejich využití v ochranných zónách, ty jsou 3 (obr.).



Obrázek 6: Rozdělení MZS

1. Obvodová ochrana

- Prostředky obvodové ochrany vymezují prostor v okolí chráněného objektu. Obvodem se nejčastěji rozumí katastrální hranice pozemků, na nichž se nachází chráněný objekt. Hranice mohou být vymezeny přírodními bariérami, jako jsou vodní toky, skalní útvary, ... Nejčastěji jsou však hranice vymezeny umělými bariérami (ploty, zdi).

2. Plášťová ochrana

- Chrání plášť budovy, jakožto i její části před vniknutím za použití všech dostupných destrukčních i nedestrukčních metod.

3. Předmětová ochrana

- Poslední stupeň ochrany, prvky předmětové ochrany mají zabezpečit uložené cenné předměty, peníze, dokumentů a jiné hmotné chráněné zájmy před odcizením nebo manipulací neoprávněnou osobou.[6]

2.2 Mechanické zábranné systémy plášťové ochrany

Pod plášťovou ochranou chápeme ochranu individuálního chráněného objektu nebo prostoru. Základním prvkem plášťové ochrany, sloužící proti vniknutí narušitele do strážného prostoru, je stavební konstrukce. Stavení konstrukce jsou přirozenými a v praxi častokrát pozapomínanými pasivními prvky ochrany.[5]

Plášť objektu je tvořený zejména:

- 1) stavebními prvky budovy
- 2) stavebními otvory

2.2.1 Stavební otvory

Jsou zajištěny otvorovými výplněmi, kterými jsou dveře, okna nebo různé vitríny či jiné prosklené plochy. Právě ty jsou nejrizikovějším místem na plášti budovy. Z policejních statistik vyplývá, že téměř polovina pachatelů, konkrétně 48%, vnikne do objektu právě dveřmi a 37% pak okny.[7] Proto je důležité těmto prvkům věnovat zvýšenou pozornost a na místo běžných dveří instalovat bezpečnostní dveře, v případě oken použít bezpečnostní skla, nebo stávající skla chránit bezpečnostní fólií, případně je doplnit o další prvky plášťové ochrany, kterými jsou mříže či rolety.

2.3 Předmětová ochrana

Jedná se o poslední zónu mechanické ochrany. Vesměs se jedná o objekty určené k uschování šperků, finanční hotovosti, cenných papírů a jiných cenností. Do skupiny předmětové ochrany řadíme především mobilní i stabilní trezory, trezorové skříně, ohnivzdorné skříně, příruční pokladny, manipulační schránky, přenosné kontejnery a kufry.

Pochopitelně všechny zmiňované prvky musejí mít kvalitní zámkový systém, který je mnohdy doplněn i elektronickým zabezpečením. Zámkový systém může mít dva typy zámků a to klíčový nebo heslový zámek.[8]

2.4 Aplikace MZS pro datová centra a informační technologie

Předchozí kapitoly nás velice stručně seznámily problematikou mechanických zábranných systémů, ale jaké je využití těchto systémů pro datová centra, nebo vůbec pro informační technologie? Tuhle otázku by mělo zodpovědět pár následujících řádků a obrázků. Nejčastěji používané prvky zabezpečení datových center a IT:

- Datové sejfy – předmětová ochrana.
- Média sejfy – předmětová ochrana.
- Zabezpečené racky – předmětová ochrana
- Datové komory – plášťová ochrana

2.4.1 Datové sejfy

Principiálně jsou datové sejfy trezory ukrývající plug&play datové úložiště a technologie správy a zabezpečení. Použitý síťový dataserver je standardní NAS se snadnou obsluhou. Systém sejfu je vybaven čidly, která sledují teplotu, vlhkost (včetně rychlosti jejich změny), kouř, napětí, otřesy a další stavy. U mnohých datových sejfů je možnost nadefinovat situace, ve kterých datový sejf zasílá poplachové zprávy e-mailem či SMS, případně se vypne a hermeticky uzavře.[9]



Obrázek 7: Datový sejf

Datové sejfy lze umístit samostatně nebo do 19" racku a spolehlivě chrání disky a data na nich i v případě, kdy je sejf vystaven extrémním teplotám okolo 950 °C. K dispozici

jsou varianty, do kterých se instaluje stávající datové úložiště, nebo s vlastním NAS serverem.

2.4.2 Média sejfy

Od datových sejfů se nijak moc neliší. Jejich úkolem je totiž zabezpečit datové nosiče před krádeží, případně před poškozením následky požáru, vytopení, elektromagnetického záření, závalu atd. Vlastně o těchto sejfách se dá říct, že jde o klasický trezor.



Obrázek 8: Média sejf

2.4.3 Zabezpečený rack

Běžný rack upravený tak, aby zamezil násilnému vniknutí. Má zesílenou konstrukci a místo klasického jednoduchého klíčového zámku je ve většině případů použit biometrický zámek. K jeho odemknutí uživatel nemusí znát žádná hesla, nebo vlastnit přístupové karty, čipy, stačí otisk jeho prstu. Díky biometrickému zámku nehrozí možnost ztráty přístupové karty, nebo prozrazení hesla. Otisk prstu má každý člověk jedinečný, přístup do takového racku tedy mají jen konkrétní pověřené osoby. Dále zabezpečený rack ochrání umístěné IT zařízení před elektromagnetickými vlnami (ze silových kabelů, pohonů, vysílačů, radarů či blesku), požárem (před horkem i zplodinami), nebo dokonce před tekoucí či tryskající vodou.



Obrázek 9: Zabezpečený rack

2.4.4 Datové komory

V podstatě se jedná o trezorovou místnost, ve které se nachází klíčová část datového centra, nebo kompletně celé datové centrum. Datová komora je samonosnou, volně stojící modulární konstrukcí, složenou ze stěnových, podlahových a stropních částí. Datové komory se vyznačují vysokým stupněm protipožární odolnosti, odolnosti proti vloupání, těsnosti před hasící a tryskající vodou a těsnosti proti prachu. Díky modulárnímu řešení (obr. 10), jsou datové komory velice flexibilní, což umožňuje v případě potřeby rozšíření provádět prakticky bez přerušení chodu datového centra.



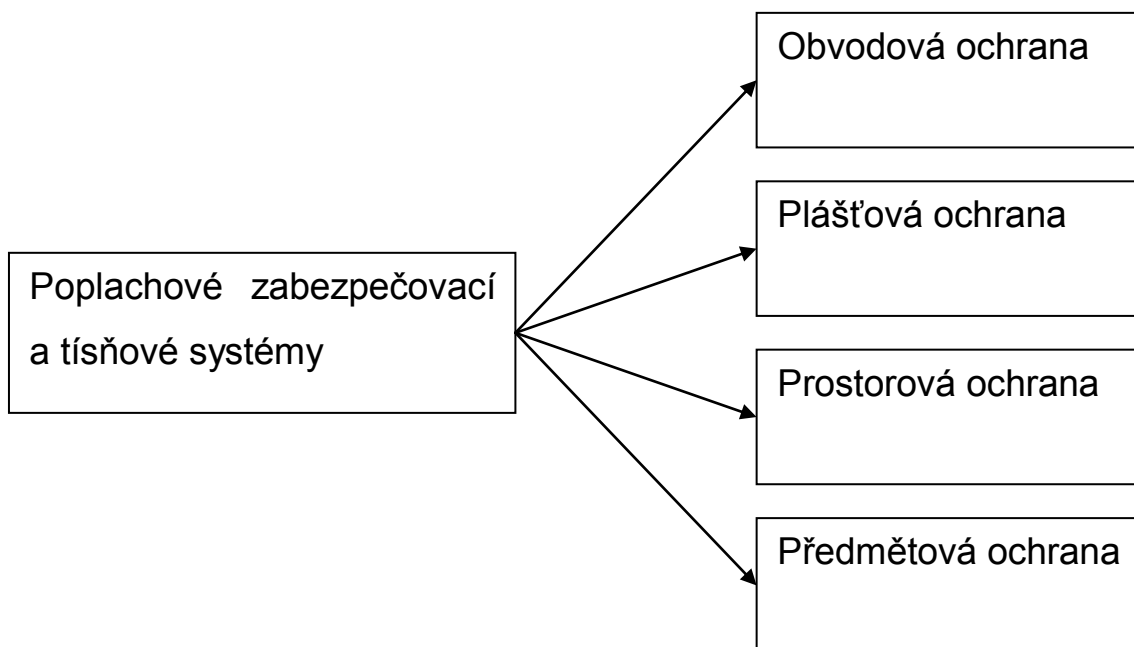
Obrázek 10: Datová komora [9]

3 POPLACHOVÉ ZABEZPEČOVACÍ A TÍSŇOVÉ SYSTÉMY

Ve zkratce PZTS, někdy se můžeme setkat s anglickou zkratkou I&HAS což znamená Intruder and Hold Up Alarm System, nebo po staru EZS (elektrické zabezpečovací systémy). I když toto označení by se již správně nemělo používat, setkáváme se s ním velice často především u prodejců a montážních firem.

Tyto systém nezabraňují vniknutí neoprávněné osoby do střeženého objektu, ale v případě, že se tak stane, o této skutečnosti informují. Mohou však podávat i tísňové informace v případě přepadení, nebo výskytu zdravotních potíží. Přestože se jejich instalací značně zvyšuje bezpečnost v chráněném objektu a jsou dnes cenově dostupné, řada lidí na ně zapomíná.

Podobně jako MZS je možné prvky (detektory) PZTS rozdělit podle chráněné zóny, ty v tomto případě rozeznáváme 4 (obr. 11). Další možné dělení je podle jejich povahy, zda vytváří vlastní pracovní prostředí, ve kterém vyhodnocují změnu sledované fyzikální veličiny – **aktivní** detektory, nebo nevytvářejí – **pasivní** detektory.



Obrázek 11: Rozdělení PZTS

3.1 Stupeň zabezpečení

Je jedním z nejdůležitějších kritérií pro poplachové systémy. Co přesně, a jaké jsou stupně zabezpečení, vymezuje norma ČSN EN 50 131-1. Říká, jaké komponenty musejí být použity a co vše je nutné chránit, aby bylo dosaženo žádaného stupně zabezpečení. Přesněji to popisují následující dvě tabulky. První ukazuje souvislost mezi stupněm zabezpečení rizikem (tab. 1), konkrétně možným narušitelem – jaké má znalosti a vybavení. Druhá tabulka pak zobrazuje co vše, a jak, je nutné zabezpečit (tab. 2).

Tabulka 1: Míra rizika

Riziko	Znalosti a vybavení narušitele	Stupeň zabezpečení
nízké	Narušitel má jen malou, nebo vůbec žádnou znalost poplachových systémů. K dispozici má jen omezený sortiment běžně dostupných nástrojů (kámen, tyč, ...).	1
nízké až střední	Narušitel má základní znalosti poplachových systémů a má k dispozici jednoduché nástroje (kleště, páčidla, ...) a přenosné přístroje (např. víceúčelový multimetr).	2
střední až vysoké	Narušitel má určité znalosti z oblasti poplachových systémů. K dispozici má úplný sortiment nástrojů a přenosných elektrických zařízení (akumulátorová vrtačka, bruska, ...).	3
vysoké	Narušitel má znalosti o funkci poplachových systémů a je schopný zpracovat podrobný plán vniknutí. K dispozici má kompletní sortiment nástrojů, přenosných elektrických zařízení a vybavení pro nahrazení komponentů poplachových systémů.	4

Tabulka 2: Stupeň zabezpečení

Zabezpečuje se	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
okna		O	O+P	O+P
vstupní dveře	O	O	O+P	O+P
ostatní otvory		O	O+P	O+P
stěny			P	P
stropy, střechy			P	P
podlahy				P
prostor místností	T	T	T	T
objekt (vysoké riziko)			S	S
<i>vysvětlivky: O – otevření P – průnik T – past</i>				
<i>S – objekty se speciální pozorností</i>				

3.2 Třída prostředí

Protože se u poplachových systémů jedná o citlivou elektroniku, je nutné dbát i na to kam se jednotlivé komponenty umísťují a následně dle toho volit vhodný komponent. Norma ČSN EN 50 131-1 rozděluje druhy prostředí do 4 tříd (tab. 3).

Tabulka 3: Třída prostředí

Třída	Název prostředí	Popis prostředí	Rozsah teplot
I.	vnitřní	Vytápěné obytné, nebo k obchodním činnostem určené prostory.	+5 °C až +40 °C
II.	vnitřní všeobecné	Přerušovaně vytápěné, nebo nevytápěné prostory (schodiště, chodby, ...)	-10 °C až +40 °C
III.	vnější chráněné	Prostory vně budov, komponenty jsou chráněny před vlivy počasí (přístřešky)	-25 °C až +50 °C
IV.	vnější všeobecné	Prostory vně budov, komponenty jsou trvale vystaveny vlivům počasí	-25 °C až +60 °C

3.3 Ostatní vlivy

Kromě vlivu typu prostředí nám na PZTS působí další vlivy, které v podstatě souvisí s daným typem prostředí a především lokalitou, ve které se střežený objekt nachází. Jsou to vlivy působící uvnitř chráněného objektu a vlivy působící vně chráněného objektu. Působením těchto vlivů může docházet k negativnímu ovlivnění správného fungování PZTS, což může způsobovat plané nebo falešné poplachy.

3.3.1 Vlivy působící vně chráněného objektu

- 1) **dlouhodobě působící faktory** (silnice, železnice, metro, parkoviště, ...)
- 2) **krátkodobě působící faktory** (výstavba)
- 3) **vlivy počasí** (vítr, deště, pobřeží, blesky)
- 4) **vysokofrekvenční rušení** (vysílače TV, R, základní stanice GSM, radary)
- 5) **sousední objekty** (vibrace, EM rušení, průmyslové objekty)
- 6) **vlivy klimatických podmínek** (místní teplota, vlhkost)
- 7) **ostatní vnější vlivy** (kulturní, sportovní akce)

3.3.2 Vlivy působící uvnitř chráněného objektu

- 1) **vodovodní potrubí** (pohyb vody – vliv na mikrovlnné detektory)
- 2) **vytápění, vzduchotechnika, klimatizace** (pohyb vzduchu – vliv na ultrazvukové detektory)
- 3) **závěsné předměty** (možnost pohybu záclony, lampy, rostliny, ...)
- 4) **výtahy** (vliv vibrací)
- 5) **zdroje světla**
- 6) **elektromagnetické rušení**
- 7) **vnější zvuky**
- 8) **domácí zvířata**
- 9) **průvan** (proudění vzduchu – přenos energie, změna teploty, ...)
- 10) **uspořádání skladovaných předmětů** (zastínění zorného pole, uvolnění předmětu)
- 11) **stavební konstrukce střežených objektů**
- 12) **umístění detektorů na zasklení**
- 13) **riziko planých poplachů u tísňových zařízení [10]**

3.4 Obvodová ochrana

Prvky obvodové ochrany jsou určeny pro střežení obvodového oplocení a venkovních prostor. Jsou důležitou součástí střežení rozsáhlých komplexů budov a prostorů. Účelem obvodové ochrany je zachytit případného narušitele včas, tedy v okamžiku, kdy ještě nepáchá trestnou činnost ve střeženém objektu. Pro aplikace v praxi se v současné době nabízí rozsáhlý sortiment prvků. Každý z nich má podle použitého fyzikálního principu své výhody a nevýhody.

Některé prvky obvodové ochrany:

- 1) mikrofonické kabely
- 2) infračervené bariéry
- 3) ultrazvukové bariéry

3.5 Plášt'ová ochrana

Detekují případný průnik pláštěm, tím jsou nejčastěji okna a dveře, v případě objektů s vysokým stupněm zabezpečení pak i stěny, stropy nebo podlahy.

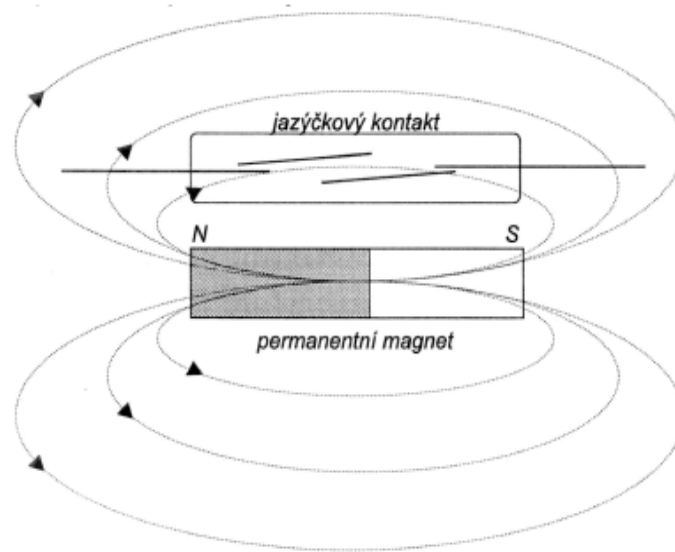
3.5.1 Magnetické kontakty

Někdy nazývané jako detektory otevření oken a dveří jsou jedny z nejpoužívanějších detektorů. Jsou tvořeny dvěma díly.

Permanentním magnetem – nejčastěji zmagnetizovaný váleček z feritu.

Jazyčkovým kontaktem – v uzavřené skleněné trubičce, naplněné ochrannou atmosférou, jsou umístěny dva kontakty z feromagnetického materiálu.

Jeden díl se montuje na rám okna (dveří) protikus pak na samotná okna (dveře). V klidovém stavu působí na jazyčkový kontakt magnetické pole permanentního magnetu, tím je kontakt sepnut (obr 12). V případě, že dojde k otevření oken nebo dveří, permanentní magnet se oddálí od jazyčkového kontaktu, čímž zmizí magnetické pole a dojde k rozepnutí kontaktu – vyhlášení poplachu.



Obrázek 12: Princip magnetického kontaktu [8]

3.5.2 Detektory rozbití skla

Jsou detektory určené k ochraně oken a dalších prosklených ploch jakou jsou například vitríny. Tříštění skla vydává velice specifický zvuk, ten se šíří hmotou skla a následně do okolí, na něj následně detektory reagují. Detektory tříštění skla lze dále rozdělit na:

- 1) pasivní kontaktní detektory
- 2) pasivní bezkontaktní detektory
- 3) aktivní kontaktní detektory. [11]

3.6 Prostorová ochrana

Je vhodným doplňkem pro plášťovou ochranu. Provázáním těchto dvou ochran se zvyšuje stupeň zabezpečení a hlavně se eliminuje riziko planých poplachů na minimum. Pro prostorovou ochranu se používá těchto detektorů:

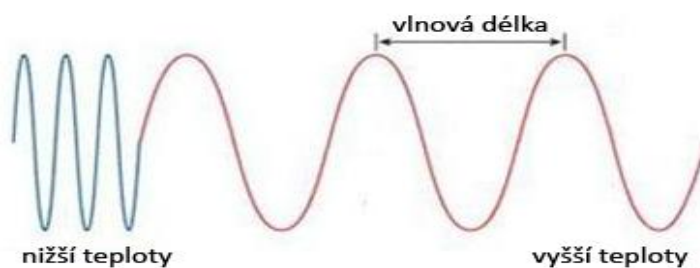
- pasivní infračervené detektory (PIR – Passive Infra Red)
- aktivní mikrovlnné detektory (MW - Microwave)
- aktivní ultrazvukové detektory (US – Ultrasonic)
- duální – kombinace PIR/MW, PIR/US – snížení rizika planých poplachů

V poslední době se na trhu objevuje i aktivní prostorová ochrana. Tou jsou zamlžovací systémy, nebo systémy s generátory bezpečnostní mlhy. Kombinace této aktivní a pasivní ochrany nám zaručuje maximální možné zabezpečení.

3.6.1 Pasivní infračervené detektory

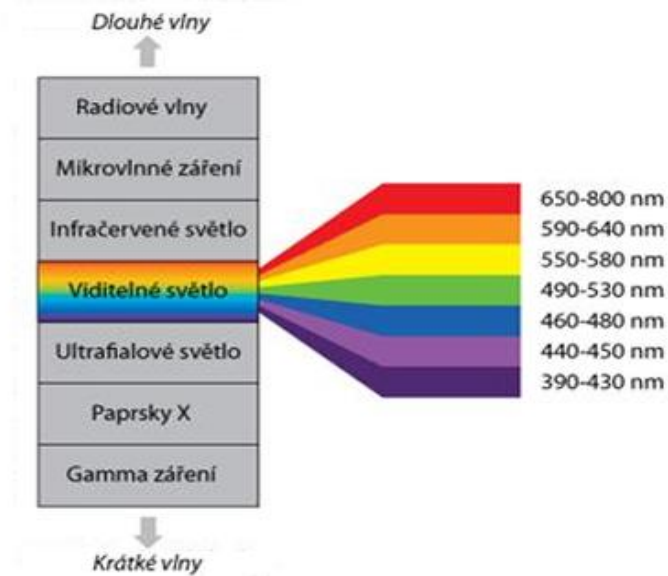
Jejich využití je opravdu široké. Využívají se nejen k detekci narušení chráněného prostoru, ale využívají se také k ovládání osvětlení a vůbec slouží ke spouštění řady dalších zařízení.

PIR pracují na principu sledování záření v infračerveném pásmu kmitočtového spektra elektromagnetického vlnění. To vyzařuje každé těleso v rozmezí teplot $-273,15\text{ }^{\circ}\text{C}$ (absolutní nula) a $+560\text{ }^{\circ}\text{C}$. Čím je teplota vyšší, tím je delší vlnová délka a opačně (obr. 13).



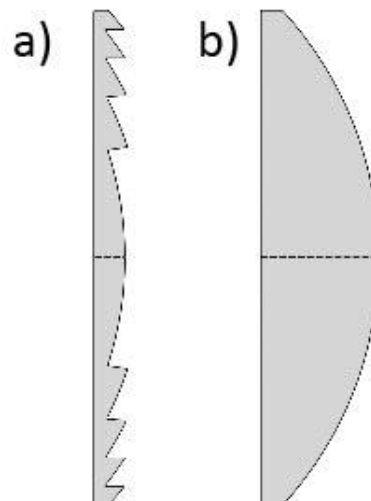
Obrázek 13: Vlnová délka

Teplota lidského těla je individuální, ale pohybuje se okolo $36\text{ }^{\circ}\text{C}$. Pro tuto teplotu je typická vlnová délka elektromagnetického záření $9,4\text{ }\mu\text{m}$, tato vlnová délka je mimo viditelné spektrum (obr. 14). Této skutečnosti se pak využívá k detekci narušení chráněného objektu.[8]



Obrázek 14: Vlnová délka viditelného spektra

Vyzařované záření zachytává pyroelement, ten reaguje pouze na změny ve svém zorném poli – pasivní detektor. To znamená, že pokud by na pyroelement trvale dopadalo záření o vlnové délce podobné vlnové délce záření emitovanému lidským tělem, pak by vstup narušitele do střeženého prostoru vyvolal jen malou změnu a nedošlo by k detekci narušení střežené zóny. Proto je střežená zóna pomocí optiky rozdělena na několik segmentů. Optika může být ve dvojitým provedení. Levnější variantou je Fresnelova čočka (obr. 15).

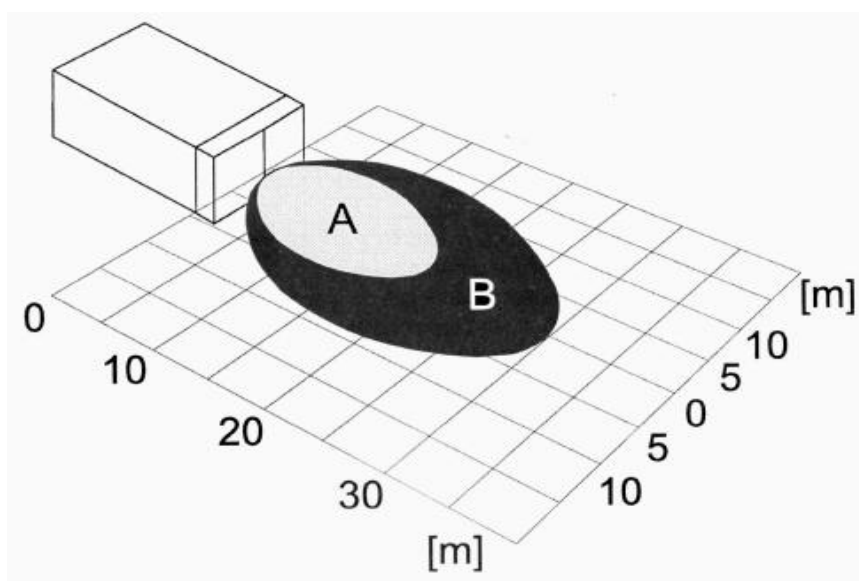


Obrázek 15: a) Fresnelova čočka b) klasická čočka

Druhou ekonomicky nákladnější, ale za to spolehlivější variantou je optika křivých zrcadel. Poskytovaný obraz chráněné zóny je přesnější a snižuje se riziko planých poplachů vyvolaných například zvířaty. Vyšší odolnosti a spolehlivosti detektorů se dosahuje také použitím tzv. černých zrcadel. Díky tomu se eliminují plané poplachu vyvolané odleskem slunce, osvětlením, atd.

3.6.2 Mikrovlnné detektory

Patří do skupiny aktivních detektorů, do svého okolí vysílají elektromagnetické záření v kmitočtovém spektru $2,5\text{ GHz}$, 10 GHz nebo 24 GHz . [11] Mikrovlnné detektory pracují na principu Dopplerova jevu, což znamená, že detektor vyhodnocuje změnu frekvence a vlnové délky. Ta se mění v závislosti na rychlosti pohybu. Pokud je tedy ve střežené zóně velice pomalu se pohybující objekt, navíc pohybuje-li se kolmo na osu detektoru, nedojde k vyhlášení poplachu. V případě, že do střežené zóny vstoupí objekt pohybující se v ose detektoru, je změna frekvence a vlnové délky odraženého elektromagnetického záření vysoká, což detektor vyhodnotí jako narušení.



Obrázek 16: Vyzařovací charakteristika - malý výkon (A), vyšší výkon (B) [8]

3.6.3 Ultrazvukové detektory

V zásadě fungují na stejném principu jako mikrovlnné detektory, jen do svého okolí vysílají ultrazvuk (20 – 45 kHz).

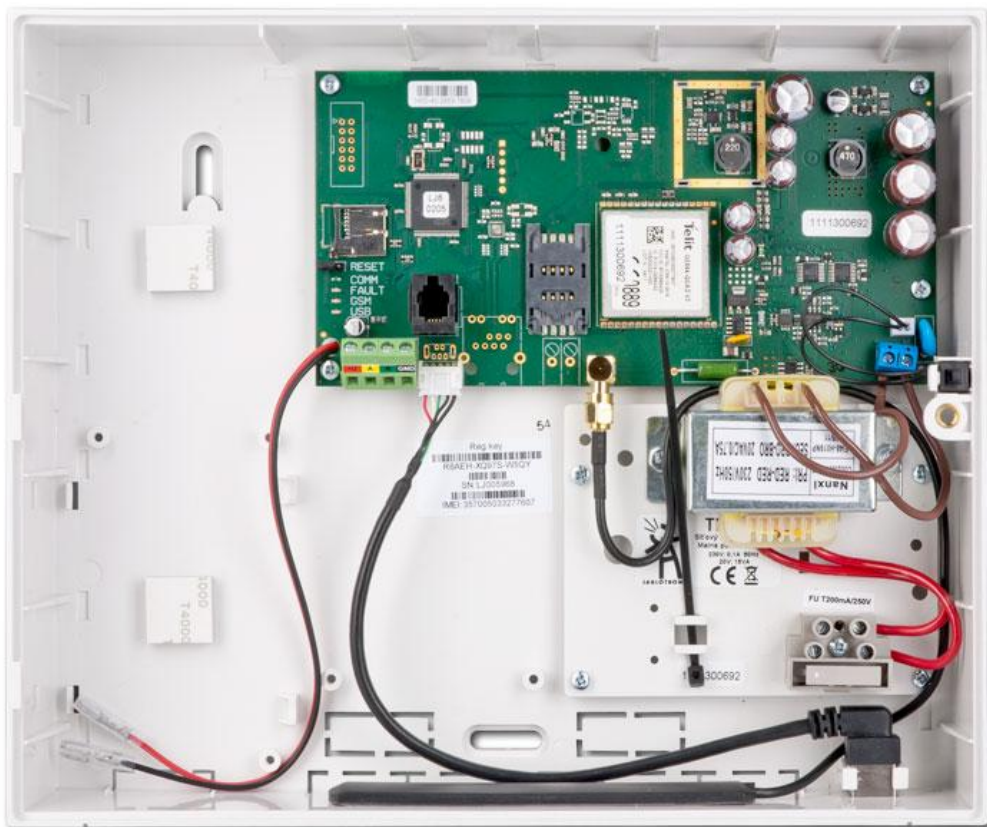
3.6.4 Duální detektory

Vzhledem k tomu, že MW a US detektory mají dobré detekční vlastnosti v případě pohybu narušitele v ose detektoru, se využívají v kombinaci s PIR detektory, které mají naopak dobré detekční vlastnosti v případě, kdy se narušitel pohybuje kolmo k ose detektoru. Další výhodou kombinování je eliminace planých poplachů.

3.7 Ústředny PZTS

Jsou takovým srdcem a mozkiem PZTS. Ústředny vyhodnocují přijatý elektrický signál od detektorů, na jehož základě vysílají poplachový signál. Ústředna je tedy elektrické zařízení, které kromě přijímání a vyhodnocování signálu od detektorů také tyto detektory napájí, ovládá další zařízení (siréna, přenosové zařízení, generátor bezpečnostní mlhy, atd.), ale také pomocí připojených ovládacích prvků (klávesnice) umožňuje nastavení systému, jeho zastřežení nebo odstřežení. Ústředny jsou tedy velice důležitým prvkem celého PZTS, proto je nutné při jejich instalaci dodržet pár zásad:

- umístění uvnitř střeženého prostoru,
- umístění na nejkratší trase od vstupu do objektu,
- umístění do prostoru s nejvyšším stupněm zabezpečení,
- zamezit možnosti sledování obsluhy ústředny,
- vyloučit přístup veřejnosti.



Obrázek 17: Odkrytovaná ústředna [12]

Podle způsobu propojení ústředny s detektory je lze rozdělit do tří skupin (systémů):

- 1) drátové (smyčkové, sběrnicové, smíšené)
- 2) bezdrátové (rádiové)
- 3) hybridní

3.7.1 Drátové ústředny

Drátové ústředny jsou propojeny s detektory pomocí metalického vedení (dráty).

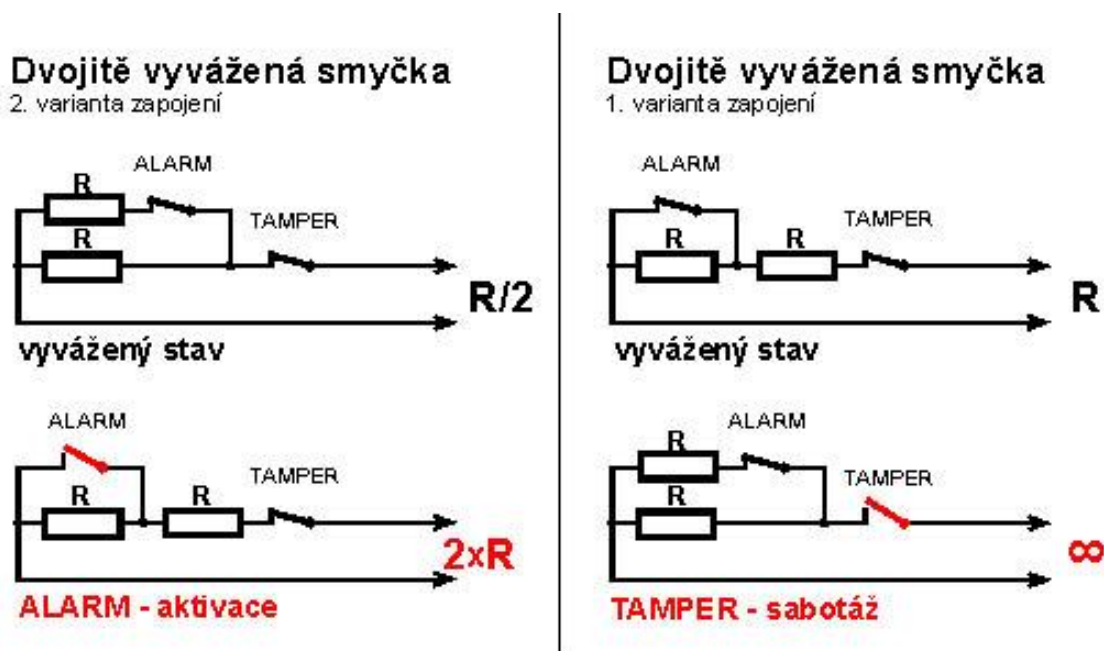
Podle způsobu zapojení metalického vedení se ústředny dále dělí na:

- 1) smyčkové
- 2) sběrnicové
- 3) smíšené.

K výhodám drátových ústředn patří nízká cena a vysoká spolehlivost. Naopak mnohdy velice rozsáhlé metalické vedení a nízké množství možností kam umístit detektory zvláště v případě historických objektů patří k nevýhodám drátových ústředn.

3.7.1.1 Smyčková

Každou poplachová smyčka ústředny je připojena k samotnému vyhodnocovacímu obvodu. Smyčka je skupina několika detektorů, nebo jiných prvků PZTS, které využívají společné vedení. Každá smyčka je zakončena zakončovacím odporem tak, aby vykazovala předepsanou hodnotu odporu pro příslušný typ ústředny. Změna odporu smyčky, způsobená aktivací detektoru nebo jiného prvku PZTS na smyčce, vede k vyhlášení poplachu.



Obrázek 18: Schéma dvojitě vyvažované smyčky

3.7.1.2 Sběrníková ústředna

Pracuje na principu komunikace po datové sběrnici, periodicky generuje adresy jednotlivých detektorů a přijímá příslušné odezvy. Délka metalického vedení takového zapojení je až stovky metrů. V případě narušení chráněné zóny oznámí, který konkrétní detektor byl aktivovaný.

3.7.1.3 Smíšená ústředna

Pracuje na principu datové komunikace ústředna - koncentrátor (sběrníkový modul smyček). Komunikace probíhá pomocí datové či analogové sběrnice. Na koncentrátory jsou detektory připojeny pomocí smyček podobně, jako je tomu u smyčkových ústředn. [12]

3.7.2 Bezdrátové ústředny

Jsou sběrnicevého typu. Sběrnice je bezdrátová, většinou v pásmu 433 MHz a 868MHz. Dosah signálu ve volném prostoru je v závislosti na použitém systému v řádech stovek metrů. Uvnitř objektů klesá tato vzdálenost přibližně na desítky metrů díky tomu, že signál musí prostupovat přes zdi a jiné překážky, čímž ztrácí na intenzitě.[8]

K jednoznačným výhodám patří bezpochyby snadná instalace díky absenci metalického vedení. S tím je spojen i minimální zásah do objektů (historické objekty, novostavby). Další výhodou je možnost rozmístění detektorů, které je velice variabilní a hlavně jej můžeme kdykoliv měnit. Bezdrátové ústředny však mají i své nevýhody, např. rušení komunikačního pásma (snížení spolehlivosti systému), ale především je to cena, která i dnes je stále vysoká. Bezdrátové systémy je tedy vhodné instalovat pouze v prostorách, které vylučují možnost použití běžných metalických vedení. Hlavním důvodem je totiž nižší spolehlivost a zvýšené nároky na pravidelnou kontrolu stavu a výměnu baterií, která v případě drátových systémů odpadá.

3.7.3 Hybridní ústředny

Do této skupiny patří většina dnes používaných ústředen. Tento typ ústředen se snaží vytežit z drátových i bezdrátových ústředen to nejlepší a minimalizovat naopak jejich nedostatky.

4 SYSTÉMY KONTROLY VSTUPU

Jsou dnes již naprosto běžnou záležitostí. Jejich uplatnění najdeme všude tam, kde je potřeba omezit vstup nepovolaným osobám, nebo k monitoringu osob. Tím se dostáváme k pojmům přístupový systém a docházkový systém. I když se dá říct, že technicky jde o jeden a ten samý systém, není tomu tak.

Přístupové systémy omezují volný a nekontrolovatelný pohyb osob ve vyhrazených prostorách a nepovolaným osobám zabraňují do těchto prostor vstup úplně. Současně jsou tyto systémy schopny monitorovat jednotlivé osoby, kde se v daný okamžik právě nachází. Díky tomuto monitoringu máme k dispozici přehled o počtu všech osob ve střeženém objektu, což je velmi výhodné v případě evakuace objektu (např. požár). Systém umožňuje i víceúrovňová přístupová práva, pomocí kterých lze nastavit omezení přístupu v určených zónách, v danou denní dobu, atd.



Obrázek 19: Ukázka systému kontroly vstupu [13]

Docházkové systémy jsou určeny ke sledování pohybu zaměstnanců během jejich pracovní doby, čímž tvoří základ pro zpracování mzdové agendy. Veškerá potřebná data jsou automaticky ukládána do databáze, tím se minimalizují chyby, které vznikají ručním

zpracováním údajů, zvláště pak u větších firem. Díky rozsáhlé databázi má vedení firmy detailní a rychlý přehled o docházce jednotlivých zaměstnanců.



Obrázek 20: Terminál docházkového systému [14]

Systémy kontroly vstupu se všeobecně skládají ze dvou základních částí. Do první se řadí všechny elektronické prvky systému, jako jsou čipové karty, řídicí jednotky a další. Druhou částí jsou prvky elektricky ovládané, to jsou prvky, které jsou ovládány např. čipovou kartou. Sem patří různé zámky, turnikety, závory, ...

4.1 Přístupové systémy

Podle velikosti a způsobu jakým systémy fungují je lze rozdělit do tří skupin:

- 1) autonomní
- 2) skupinové
- 3) globální - síťové

4.1.1 Autonomní

Ke správnému fungování takového systému není potřeba specializovaný obslužný software. Pracují zcela nezávisle na počítačích nebo jakékoliv jiné řídicí jednotce. Nastavení,

naprogramování autonomního systému je snadné a rychlé, využívá se k tomu hlavní ovládací prvek – Master karta.

Používají se zejména:

- 1) vchody domů
- 2) garáže, dílny
- 3) náhrada klíčů tam, kde je více uživatelů, vyšší bezpečnost, odolnost

4.1.2 Skupinové

Jsou připojeny na sběrnici (RS485) a následně k počítači, na kterém běží specializovaný ovládací software k zadávání všech přístupových práv a dalších parametrů pro jednotlivé dveře, případně osoby individuálně.

4.1.3 Globální - síťové

Tyto přístupové systémy jsou spojením dvou předchozích k tomu je možnost systém připojit na místní síť LAN a řídit jej i prostřednictvím internetu nebo intranetu.[13]

4.2 Elektronické prvky

Elektronická část slouží k ovládání a řízení systému. Skládá z několika dalších prvků, kterými jsou:

- 1) čipy, resp. karty,
- 2) čtečky čipů, resp. karet,
- 3) řídicí jednotky,
- 4) napájecí zdroj,
- 5) kabelový rozvod.

4.2.1 Čip

Slouží k identifikaci oprávněného uživatele. Dnes jsou nejčastěji používány bezkontaktní RFID čipy. Ty se vyrábějí v mnoha variantách od přívěsku ke klíčům po kreditní karty. Čtecí vzdáleností od čtečky je pouze několik centimetrů.



Obrázek 21: Čip v podobě přívěsku ke klíčům

4.2.2 Čtečky

Na našem trhu jsou k dostání systémy používající univerzálních rozhraní, stejně tak lze narazit na systémy, u kterých výrobci používají vlastní rozhraní. Proto je nesmírně důležité při výběru prvků věnovat pozornost právě čtečkám, konkrétně způsobu komunikace mezi čtečkou a řídicí jednotkou. V případě vlastního komunikačního rozhraní riskujeme, že výrobce v lepším případě přestane dané komunikační rozhraní podporovat z důvodu vývoje nového, nebo v horším případě zanikne sám výrobce.



Obrázek 22: Čtečka čipové karty s klávesnicí [14]

Univerzálním rozhraním běžně a často používaným je rozhraní označené jako *Wiegand 26bitů*. Méně často se lze setkat s 32 bitovou verzí, ale i dalšími jako jsou BC-Link nebo Clock&Data. Pokud bude použito tohoto rozhraní, budeme mít jistotu, že systém

je schopný fungovat dlouhodobě. V případě poškození některé ze čteček ji tak snadno vyměníme bez větších zásahů do systému.

4.2.3 Řídicí jednotka

Je mozkiem systému, přijímá údaje ze čtečky, porovnává je s údaji uloženými v databázi a na základě toho vysílá signál ovládanému zařízení k povolení vstupu, pokud byla nalezena shoda. Taktéž eviduje historii průchodů – který čip byl kdy, případně kde, použit.

V menších systémech je řídicí jednotka samostatným elektronickým zařízením. Mnohem pohodlnější administrace systému je v případě, kdy řídicí jednotku nahrazuje běžné PC, na kterém běží specializovaný software k ovládnání systému.



Obrázek 23: Personalizační čtečka

Pro snadné a rychlé zadávání nových čipů z místa připojení počítače je ideální, aby zde byla tzv. personalizační čtečka (obr. 23).

4.2.4 Napájecí zdroj

Napájí všechny prvky nejčastěji stejnosměrným napětím 12V. Součástí je i záložní bezúdržbový akumulátor, ten zajišťuje v případě výpadku síťového napájení řádnou funkci systému.

4.2.5 Kabelové rozvod

Většinou jsou řešeny sběrnici, propojující řídicí jednotky a taky každou řídicí jednotku s její čtečkou a zámkem.[15]

4.3 Elektricky ovládané prvky

K často používaným patří samo-zamykací elektromechanické zámky. Jako jejich alternativa mohou být k zamykání používány tzv. přídržné elektromagnetické zámky. Jde o elektromagnety s přídržnou silou cca 300 kg a více. Oproti samo-zamykacím zámkům jsou podstatně levnější a mají vysokou spolehlivost, ta je dána tou skutečností, že mají jen minimum pohyblivých dílů.

Dalším ovládaným prvkem, se kterým se můžeme často setkat, jsou turnikety. Jsou to kompaktní zařízení určená pro rychlé řízení přístupu osob do střežených prostor (a nejen tam). Mohou být umístěny uvnitř objektu (recepce) nebo vně (vrátnice). Elektromechanická konstrukce turniketů zaručuje dlouhou životnost a jejich modifikace dovolují široké využití.

5 PROTIPOŽÁRNÍ OCHRANA

O tom jaké škody dokáže požár napáchat, snad není třeba diskutovat. Kromě naprosté destrukce všeho, co se v jeho okolí nachází, je zde pro firmy ještě jeden mnohem závažnější problém. Jak již bylo několikrát v předchozích kapitolách řečeno, jsou to data. Taktéž jsme si řekli, pomocí jakých prostředků lze škody napáchané požárem na našich datech minimalizovat. Avšak tím úplně nejefektivnější způsobem, jak zabránit požáru v napáchání škod, je mu předcházet, ale také rychlý a účinný zásah. Toho lze dosáhnout jen tehdy, když budeme včas informováni o požáru.

5.1 Elektrická požární signalizace

Systém elektrické požární signalizace (dále jen EPS) tvořen ústřednou EPS, hlásiči požáru a koncovými případně ovládacími zařízeními. Úkolem EPS je informovat uživatele o vzniku požáru a to akusticky nebo opticky přímo v objektu, nebo pomocí zařízení pro dálkový přenos je tato skutečnost signalizována přímo u hasičského záchranného sboru. Systém EPS je schopný odhalit požár již v jeho latentní podobě, tj. dřív, než se objeví první plameny. Prvním příznakem hrozícího požáru je kouř, ten se objeví dříve než zvýšená teplota. Právě tato fáze, kdy dochází teprve k doutnání, nebo případně již vypukl požár, který se nachází v I.fázi (počátek požáru - hoří jen hořlavé látky v ohnisku požáru) je ideální k zahájení hasebních prací.

K včasnému zjištění požáru se používají detektory založené na různých fyzikálních principech (teplota, volné částice obsažené ve vzduchu,...). Výhodou EPS je propojení s dalšími systémy jako jsou stabilní hasicí zařízení (dále jen SHZ) nebo jiná zařízení zabráňující šíření požáru (protipožární větrací zařízení, požární uzávěry otvorů, ...).

5.1.1 Základní rozdělení EPS

Podobně jako ústředny PZTS lze rozdělit i EPS do tří skupin (v závorce je uvedena podobnost s ústřednami PZTS):

1. **Konvenční** – (smyčkové) do smyčky lze připojit několik hlásičů, nevýhodou je pokud dojde k poplachu, víme pouze, že na smyčce je některý (nebo více) hlásičů v poplachu ale nejsme schopni zjistit který.

2. **Adresovatelné** – (sběrníkové) o tom, zda bude vyhlášen poplach, rozhodne hlásič, ten vyšle signál ústředně, která díky adrese hlásiče ví, ve kterých místech došlo k vyhlášení poplachu.
3. **Analogové** – (sběrníkové) jsou podobné předchozími typu hlásičů, též mají svou adresu, jen s tím rozdílem, že sledují určité fyzikální veličiny. Zjištěné hodnoty odesílají ústředně a ta rozhodne o poplachu.[16]

5.2 Součásti systému EPS

Skládá se z ústředny EPS, tlačítkových a samočinných hlásičů, požárního poplachového zařízení, požárních kabelů, adaptérů a dalšího příslušenství.[8]

5.2.1 Ústředna EPS

Je elektrické zařízení, které přijímá a vyhodnocuje elektrické signály požárních hlásičů, signalizuje a vysílá informace o vlastním provozním stavu, ovládá doplňující zařízení EPS a přímo či nepřímo ovládá zařízení bránící rozšíření požáru, popř. provádějící protipožární zásah.[16]



Obrázek 24: Ústředna EPS [17]

5.2.2 Hlásiče požáru

Zařízení, které reagují na signál detektoru a vytvářejí výstupní elektrický signál, který je odeslán ústředně EPS, a to buď samočinně, nebo manuálně osobou. Ústředna pak na základě přijatého signálu od hlásiče následně vyhlásí poplach. Jejich základní rozdělení je:

- 1) tlačítkové hlásiče
- 2) samočinné hlásiče
- 3) ionizační hlásiče kouře
- 4) optické hlásiče kouře
- 5) teplotní hlásiče

5.2.2.1 Tlačítkové hlásiče

Jsou manuální hlásiče požáru. Signál pro ústřednu je vyslán při stisknutí tlačítka. To se nachází za ochranným sklíčkem. Tento typ hlásičů se umísťuje na viditelná místa kde je vysoká frekvence pohybu osob, ideálně ve směru únikové cesty.



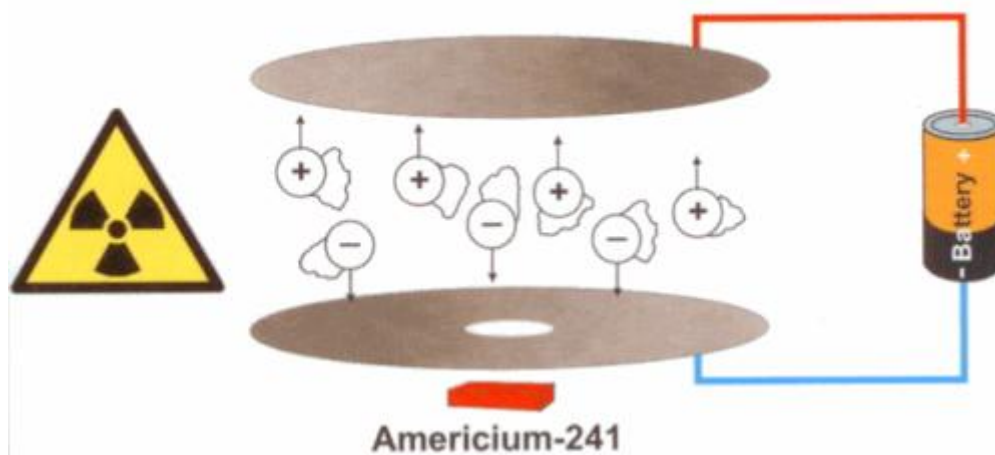
Obrázek 25: Tlačítkový hlásič

5.2.2.2 Samočinné hlásiče

Též se s nimi můžeme setkat jako s autonomními hlásiči. Na základě změny sledované fyzikální veličiny upozorní na poplach akustickým signál, případně doplněným o optickou signalizaci. Hlásiče reagují na zvýšenou teplotu nebo na přítomnost kouře.

5.2.2.3 Ionizační hlásič kouře

Obsahuje ionizační komoru, ve které se nachází malé množství radioaktivního Americia 241. Díky vyzařovaným alfa částicím není hlásič pro člověka nebezpečný, alfa částice totiž zastaví list papíru nebo několik centimetrů vzduchu. Nicméně přímá manipulace s Americiem se nedoporučuje. Díky ionizaci vzduchu v komoře dochází k vytvoření volných částic, ty z ionizovaného vzduchu vytvářejí slabý vodič (obr). V případě kdy do ionizační komory vnikne kouř, čímž dojde k navázání těchto volných částic a následně ke snížení elektrického napětí v komoře. Protože vodivost vzduchu ovlivňují i další faktory, jako je teplota nebo vlhkost, využívá se v některých případech dvou ionizačních komor. Jedna je otevřená, do té vniká okolní vzduch, druhá je polozavřená, tzv. referenční komora.



Obrázek 26: Princip ionizační komory

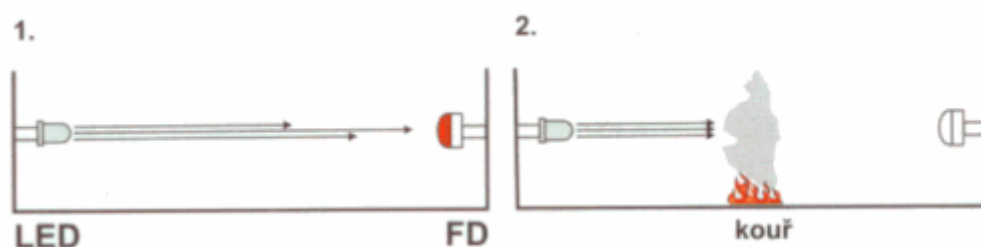
V referenční komoře se nachází opět malé množství Americia. Připojením k napájení začne referenční komorou protékat elektrický proud. Ve chvíli kdy do otevřené komory vnikne kouř, dochází ke stejnému ději, jako u hlásiče s jednou komorou, tedy snížení napětí v koře a s tím spojené snížení množství elektrického proudu. Tím je rozdíl napětí mezi jednotlivými komorami vyšší. Pokud toto napětí překročí stanovenou mez, dojde k vyhlášení poplachu.

Vzhledem k poločas rozpadu Americia 241, který je přibližně 430 let se od používání tohoto typu hlásičů upouští po celé Evropě – ekologické důvody.

5.2.2.4 Optický hlásič kouře

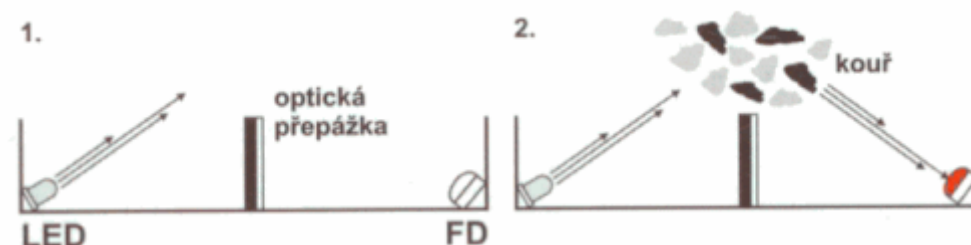
Využívá vlastností optického prostředí. Základem je zdroj světla, tím bývá pulzující LED dioda umístěná uvnitř hlásiče v labyrintu, do kterého nepronikne okolní světlo. Kouř sem však může vniknout naprosto bez problému. Tady se využívá dvou principů.

- 1) Paprsek světla vycházející ze zdroje dopadá neustále na fotodiodu (analogie infračervených bariér), ve chvíli, kdy do labyrintu vnikne kouř, začne se paprsek světla lámat a nedopadá na fotodiodu o dostatečné intenzitě (obr. 27) – spínání tmou.



Obrázek 27: Spínání tmou

- 2) Mezi zdrojem světla a fotodiodou je trvale překážka, paprsek světla tak nedopadá na fotodiodu. Pokud ovšem vzduch v labyrintu bude obsahovat kouř, dojde opět k lomu paprsku světla vyslaného zdrojem. Pak stačí jen nízká intenzita světla dopadajícího na fotodiodu k vyhlášení poplachu (obr. 28) – spínání světlem.



Obrázek 28: Spínání světlem [18]

5.2.2.5 Hlásiče teplot

Sledovanou fyzikální veličinou je teplota. Hlásič tedy reaguje na překročení maximální teploty (absolutní) nebo rychlostí nárůstu teploty (diferenciální). Protože každá z možností je sama o sobě ne příliš spolehlivá, využívá se kombinace. Pokud by při požáru teplota narůstala dostatečně pomalu, hlásič by nezareagoval, nebo naopak pokud bychom zapnuli vytápění místnosti, může diferenciální hlásič vyhlásit poplach. Na druhé straně pokud budeme sledovat jen maximální teplotou, může být pro včasný zásah pozdě, protože ve chvíli, kdy je teplota okolního vzduchu např. 60 °C je požár již značně rozšířený. Proto pro včasnější vyhlášení poplachu a redukci planých poplachů se využívají v kombinaci.

5.3 Stabilní hasicí zařízení

Stabilní hasicí zařízení (dále jen SHZ) na rozdíl od mobilní požární techniky je pevně zabudované v chráněném objektu. Z pevně zabudovaného zdroje se hasicí prostředek dopravuje do potrubního rozvodu s ukončenými výstřikovými prvky. V činnost se uvádí automaticky nebo ručně. Podle použitého hasiva se SHZ dělí na:

1) vodní

- sprinklerová hasicí zařízení
- sprejová hasicí zařízení
- mlhová hasicí zařízení

2) pěnová

- hasicí zařízení na těžkou pěnu
- hasicí zařízení na střední pěnu
- hasicí zařízení na lehkou pěnu

3) plynová

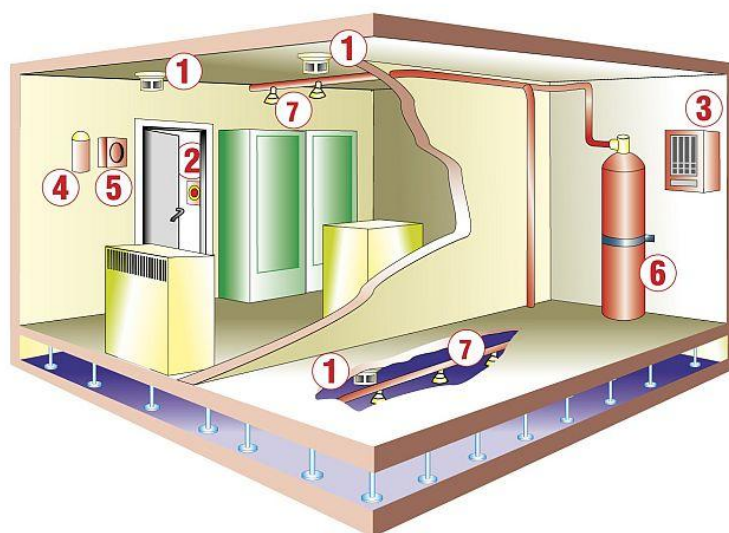
- hasicí zařízení CO₂
- hasicí zařízení na inertní plyny

4) prášková

5.3.1 Plynová SHZ

Tato hasicí technika se používá převážně tam, kde nelze použít standardní hasicí systémy s vodou či pěnou, nebo tam, kde by voda způsobila větší škodu na majetku. Plynové SHZ jsou tedy jasnou volbou pro datová centra.

Dříve se jako hasivo používal halon, ten je však díky své škodlivosti dnes zakázán a je nahrazen jinými inertními plyny. Princip hašení inertním plynem spočívá ve snížení hladiny kyslíku z běžných 21% na zhruba 10%. Při tak nízké hladině není ve vzduchu dostatek kyslíku potřebného k hoření, nicméně je to stále dostatečné množství kyslíku, aby nebylo ohroženo lidské zdraví.



Obrázek 29: Schéma SHZ

Princip činnosti SHZ (obr. 29): Při zjištění požáru automatickým hlásičem (1), resp. při spuštění ručního hlásiče (2) se přes požární centrálu (3) spustí poplašná zařízení (4/5). Po uplynutí doby, která je stanovena pro daný objekt, se elektricky otevře láhev s hasicím prostředkem (6) a hasivo začne proudit tryskami (7) do místnosti. [19]

6 ZDROJE NEPŘERUŠOVANÉHO NAPÁJENÍ

Bezproblémový provoz Datových center je nemyslitelný bez zdrojů nepřerušovaného napájení mnohdy jen zkráceně UPS (Uninterruptible Power Systems). Všechna datová centra, počínaje malými firemními datovými centry, by zřejmě měly vážné problémy, kdyby zůstaly bez elektrického napájení. Ze statistického hlediska to rozhodně není tak nepravděpodobné, jak se snad může zdát. Při dostupnosti napájení 99,98 % je třeba počítat průměrně se 105 minutami výpadku proudu ročně. V této statistice ovšem nejsou brány v potaz různé mimořádné události. Většina datových center si takové riziko nemůže dovolit, není pro ně tedy jiná možnost, než se pojistit a pořídit si UPS.

Vedle samotného výpadku proudu je však třeba zohlednit i jiné poruchové faktory, které mohou vést ke škodám na vybavení IT, pokud v síti nejsou nainstalována žádná zařízení pro zajištění nepřerušovaného napájení nebo na ochranu proti přepětí. Podle odhadů odborníků lze kolem 60% všech problémů s IT přičíst poruchám napájení. V ideálním případě by mělo být k dispozici elektrické napětí ve tvaru čisté sinusoidy. Skutečnost je však úplně jiná. Střídavé napětí dodávané přímo ze sítě je nespojitě a vykazuje řadu nepravidelností. Ke snížení kvality napájení může docházet i v případě, kdy uvnitř budovy jsou zařízení, která při svém spuštění mohou způsobit proudový náraz. K takovým zařízením patří např. výtahy, ty mohou způsobit natolik velké proudové zatížení, že oslabí dodávku proudu do ostatních připojených spotřebičů. K nejdůležitějším problémům s elektrickým proudem patří přepětí, vysokonapěťové špičky, spínací špičky, podpětí, vysokofrekvenční rušení, zkrat, výpadek sítě, elektrický šum ve vedení nebo harmonické vlny. Všechny tyto zmiňované faktory mohou být příčinou vážných problémů.



Obrázek 30: Jednoduchá jednotka UPS

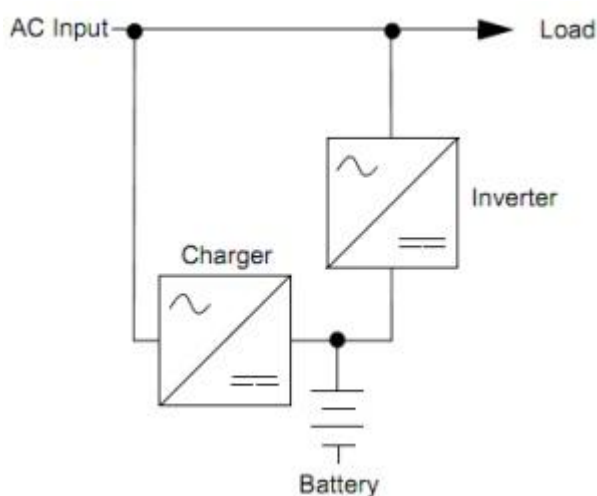
Podle doc. Ing. Jaroslava Žáčka, CSc. je zdroj nepřerušovaného napájení UPS definován jako: „kombinace měničů, spínačů a zásobníků energie, např. baterií, vytvářející výkonový systém pro udržení kontinuity napájení zátěže při poruše napájecí sítě.“[20]

Jednotka UPS se standardně skládá z usměrňovače, střídače a baterie. V některých případech je možné, že střídač a usměrňovač jsou realizovány jako jeden prvek, obousměrný měnič. Jednotky UPS lze použít samostatně, nebo je možné je vzájemně propojit a vytvořit tak celý systém, který může být paralelní, nebo redundantní. Systémům UPS se ale budeme věnovat později.

6.1 Typy UPS

6.1.1 Off-line

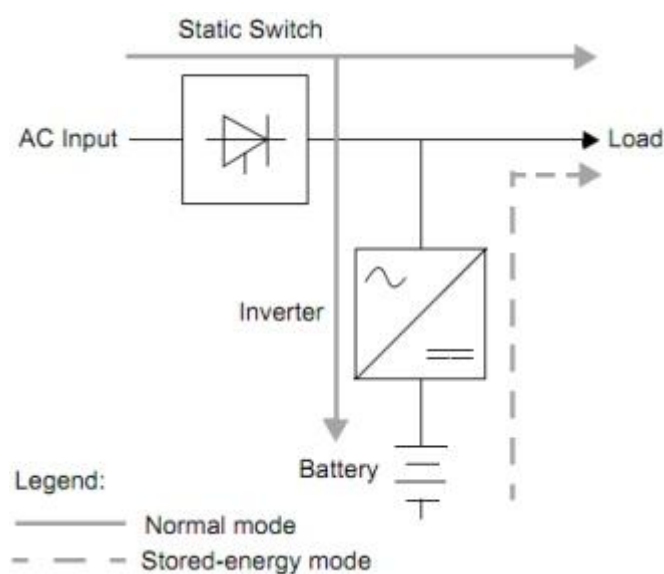
Někdy je možné se setkat s označením VFD (Voltage and frequency dependent – napětově a frekvenčně závislé). Tento typ UPS je schopný bez problémů překlenout krátkodobý výpadek napájení zátěže ze sítě a to v rozmezí 5 – 10 minut. V případě off-line typu můžeme říct, že zátěž, i když je přímo připojena k UPS, je vlastně napájena ze sítě. V „bezporuchovém“ stavu, kdy je napájení ze sítě v pořádku, je střídač vyřazen. Procházející napětí je upravováno pouze pasivními filtry, ty ale nedokážou eliminovat veškeré problémy s napájením v rozvodné síti. Přepínání mezi síťovým a bateriovým provozem je uskutečňováno pomocí relé, v průběhu přepínání dojde ke krátkému odstavení, řádově v milisekundách, napájení zátěže.



Obrázek 31: Schéma off-line UPS

6.1.2 Line-interactive

Též pod označením VI (Voltage independent – napěťově nezávislé) jsou záložní zdroje, jejichž konstrukční a technologické provedení snižuje opotřebení baterie. Toho je dosaženo použitím regulačního transformátoru, ten dokáže vyrovnávat krátkodobé anomálie v rozvodné síti, jako jsou podpětí, přepětí, nebo rázy, tím nedochází k nadměrnému zatěžování baterie. Podobně jako u off-line typu i zde dochází k odpojení napájení zátěže při přepínání ze síťového na bateriový provoz. Ovšem doba, po kterou je zátěž odpojena, je zhruba poloviční oproti off-line typu.



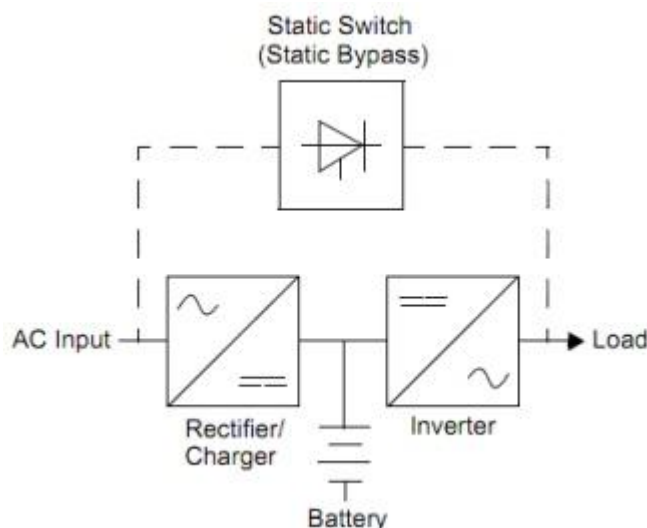
Obrázek 32: Schéma line-interactive UPS

6.1.3 On-line

Nebo také VFI (Voltage and frequency independent – napěťově i kmitočtově nezávislé). Aby se dosáhlo této nezávislosti je nutné trvalé zapojení baterie, díky tomu se však snižuje její životnost, ale na výstupu máme přesnou hodnotu napětí. Dále se využívá dvojí konverze napětí. To se nejprve usměrňuje na stejnosměrné, které je pak střídačem opět rozkmitáno na střídavé napětí o přesném kmitočtu. Díky tomu dostáváme na výstup napětí s přesně takovými parametry, jaké jsou pro bezpečný provoz zátěže potřebné. Vyrovnávají se tak veškeré nedostatky v napájecí síti.

Zařízení typu on-line může pracovat ve 3 režimech:

1. Síťový provoz – pokud vstupní napětí má správné parametry, v tolerančních mezích, je usměrňováno a teče do stejnosměrného meziobvodu. Odtud je směřováno do střídače, který z něj opět dělá střídavé napětí, případně se směřuje do akumulátorů baterie, nejsou-li nabity na 100%.
2. Bateriový provoz – tento případ nastává tehdy, pokud jsou parametry vstupního napětí mimo stanovené tolerance. V tuto chvíli je usměrňovač odstaven a stejnosměrné napětí je odebíráno z akumulátorových článků baterie. Následující proces je pak stejný, jako u síťového provozu.
3. By-pass



Obrázek 33: Schéma on-line UPS [21]

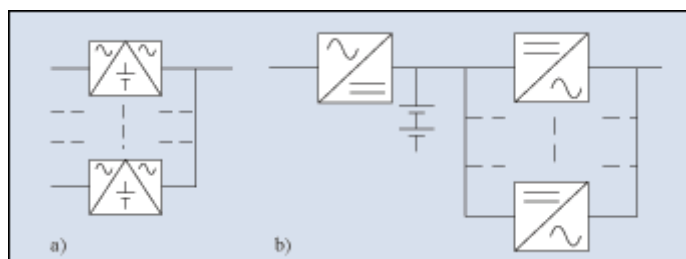
6.2 Systémy UPS

Jak bylo zmíněno při definování UPS, je možné vzájemné propojení mezi jednotkami. Díky tomuto propojení jednotek UPS pak vznikají systémy, ty mohou být:

1. Prosté – nejjednodušší způsob zapojení, pouze jedna jednotka typu off-line, line interactive, nebo on-line (viz obr. 30 – kapitola 6).
2. Paralelní
3. Redundantní

6.2.1 Paralelní

Jak napovídá samotné pojmenování systému, jde o paralelní zapojení několika UPS jednotek. Jejich střídače pracují synchronně, čímž se dosahuje mnohem vyšších výkonů. Kromě klasického paralelního zapojení je zde také varianta částečného paralelního zapojení (obr. 34). To znamená, že systém má pouze jeden usměrňovač a jeden stejnosměrný obvod a střídače systému jsou zapojeny paralelně. Obě varianty je možné ještě doplnit obtokem, ale především je takový systém provozován jako jedna vlastní jednotka UPS.



Obrázek 34: Paralelní zapojení jednotek UPS

6.2.2 Redundantní

Neboli jinak nadbytečný je takový systém, který je tvořen několika jednotkami UPS, v zásadě však minimálně dvěma. Tohoto systému zapojení UPS jednotek se využívá ke zvýšení spolehlivosti systému. Možnosti zapojení systému jsou dvě a to pohotovostní zapojení a redundantní paralelní.[20]

6.3 Komunikační rozhraní

Důležitým prvkem u UPS jednotek je komunikační rozhraní. Úkolem komunikačního rozhraní je právě komunikace mezi UPS a připojeným zařízením (PC, NAS, a další IT zařízení). Při výpadku proudu je pak záložní zdroj schopen zálohované zařízení bezpečně vypnout. Pokud UPS jednotka komunikační port neobsahuje, bezpečné vypnutí zbývá na uživateli, který je upozorněn akustickým signálem. [22]

7 KLIMATIZACE A VZDUCHOTECHNIKA

Klimatizace a vzduchotechnika mají za úkol ochránit datová centra před přehříváním, vysoké teploty totiž mají negativní vliv na výkon a hlavně na životnost IT technologií. Snížená životnost znamená vyšší riziko ztráty dat a tím způsobenou škodu.

Pod pojmem klimatizace se však ukrývá víc, než jen zařízení, které vyrábí chladný vzduch. Klimatizace tedy můžeme rozdělit do dvou základních skupin:

- 1) klimatizace komfortní
- 2) klimatizace přesné

7.1 Komfortní klimatizace

Slouží pro klimatizování místností a prostor určených k pobytu osob. Tento typ klimatizace má za úkol nám poskytnout lepší teplotní komfort. Tuto skupinu klimatizací však můžeme dále dělit a to podle provedení, nebo podle toho, pro jak velké prostory jsou určeny.

- 1) klimatizace pro domácnosti
- 2) klimatizace komerční

7.1.1 Split systém

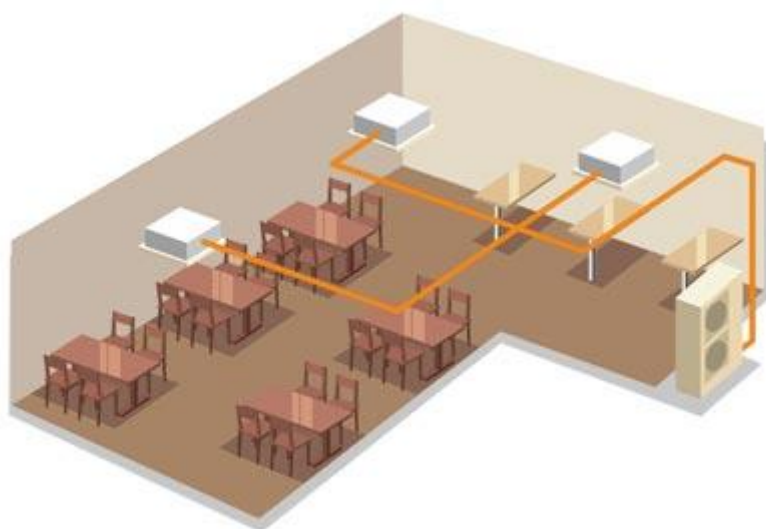
Název systému vychází z anglického slovíčka split, neboli rozdělit. Systém klimatizace je rozdělen na dvě části. Na vnitřní a venkovní klimatizační jednotku. Tyto klimatizační jednotky jsou mezi sebou vzájemně propojeny potrubím, v němž koluje chladivo.[24]

Vnitřní jednotka je složena z výparníku, ventilátoru a řídicího systému s čidly teploty. Výparník slouží k odpařování kapalného chladiva, při odpařování dochází k odebírání tepla okolí, v tomto případě výparníku, který se tak ochlazuje. Do prostoru s ochlazeným výparníkem se nasává vzduch z místnosti skrze filtr, aby se zamezilo vniknutí pevných prachových částic. Vzduch je tak chladným výparníkem ochlazován, respektive zde dochází k výměně tepla mezi výparníkem a nasátým vzduchem. Ten ohřívá výparník,

předává mu své teplo a naopak výparník tím, že odebírá teplo vzduchu, jej tím ochlazuje. Následně je vzduch opět vháněn do místnosti.

Venkovní jednotka, složená z kompresoru, expanzního ventilu a kondenzátoru s ventilátorem, slouží k tomu, aby plynné chladivo bylo přeměněno zpět na kapalné. Toho se dosahuje tak, že plynné chladivo odpařené ve výparníku (vnitřní jednotka) je přiváděno potrubím pro chladivo. Ve venkovní jednotce se ohřáté chladivo kompresorem stlačí a posílá se do kondenzátoru. Ten je působením venkovního vzduchu ochlazován. Aby se zvýšila efektivita ochlazování kondenzátoru, používá se ventilátor. Tím dochází ke kondenzaci chladiva a jeho opětovnému zkapalnění. Kapalné chladivo je potrubím přiváděno zpět do výparníku vnitřní jednotky, čímž je chladicí okruh uzavřen. [25]

Multi split systém - jde principiálně o podobný systém jako je split, jen s tím rozdílem, že umožňuje připojení více (2-5) vnitřních jednotek na jedinou venkovní klimatizační jednotku. [24]



Obrázek 35: Split systém

7.2 Přesná klimatizace

Sloužící k vytvoření optimálního prostředí pro IT technologie, telekomunikační zařízení, klimatizaci laboratoří a výrobních prostor. V klimatizovaném prostoru se nepředpokládá trvalý výskyt osob. A jak je již dobrým zvykem, i tuto kategorii můžeme dál rozdělit.

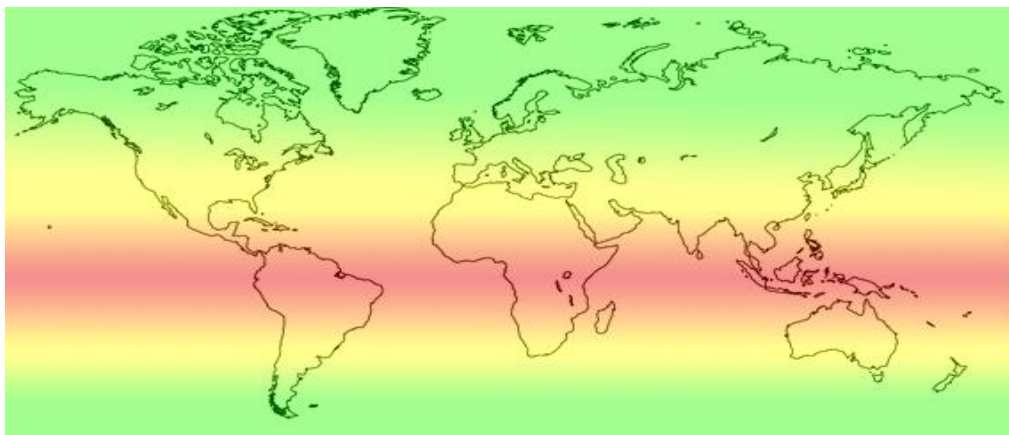
- 1) Klimatizace pro IT technologie a telekomunikace
- 2) Klimatizace s úzkými tolerancemi teploty a vlhkosti a čisté prostory

Přesné klimatizace můžeme rozdělit podle jmenovitých výkonů klimatizačních jednotek na tři kategorie klimatizačních jednotek vhodných pro:

- 1) malá datová centra – nízké výkony 1 – 15 kW
- 2) střední datová centra – výkon 12 – 300 kW
- 3) velká datová centra – výkony nad 1500 kW [23]

7.2.1 Freecooling

Pro snížení ekonomických nákladů na energii a šetření energií se využívá při chlazení tzv. freecooling, neboli chlazení venkovním vzduchem. Pro využití freecoolingu je nutné, aby venkovní vzduch byl alespoň o teplotě 18°C a nižší. Tato metoda s sebou přináší obrovskou možnost úspory nákladů na provoz datového centra. Ovšem jsou s ní spojeny i problémy a možné komplikace. Při využití freecoolingu je vháněn do chlazeného objektu, nebo místnosti velký objem venkovního vzduchu. Proto je nutné rozšířit tolerance teploty, ale hlavně vlhkosti. Aby se předcházelo těmto problémům, využívá se metoda tzv. nepřímého freecoolingu. Pro přenos tepla mezi vnitřním teplým a vnějším chladným vzduchem se používá kapalné médium (30% glykol). Sice zde není taková úspora na energii, nicméně nedochází k provětrávání klimatizovaného prostoru venkovním vzduchem, a tím k problémům s filtrací prachu a především udržení požadované vlhkosti.



Obrázek 36: Oblasti pro freecooling

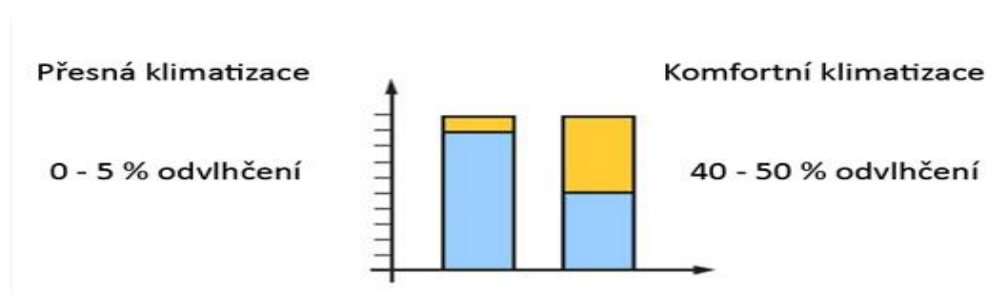
Oblasti, které jsou nejméně vhodné pro využití freecoolingu, díky svému klimatu se na následujícím obrázku (obr. 36) nacházejí v červené zóně, naopak oblasti vhodné a ideální k využití freecoolingu leží v zóně zelené.

7.3 Návrh klimatizace datových center

7.3.1 Návrh chlazení malých datových center

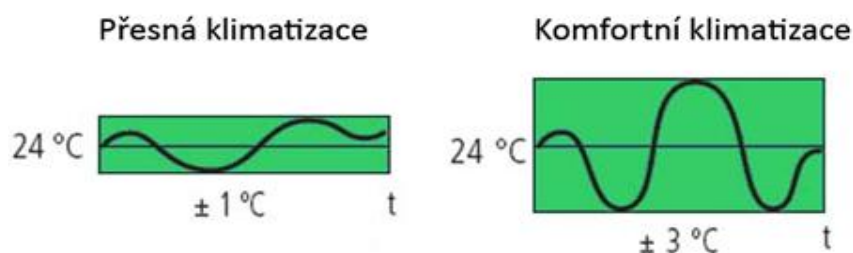
Při návrhu je nutné počítat nejen s tepelnou zátěží vyzářenou IT technologiemi, ale je důležité vzít v úvahu i teplo pronikající do datového centra z okolí, ať už se jedná o oslunění okny, prostupem stěnami a stropem z vnějšího prostředí, ale i prostup tepla z přilehlých místností. Další důležitou veličinou je vlhkost, ta je důležitá pro předcházení problémů se statickou elektřinou. Jak bylo řečeno dříve, je vhodné volit přesné klimatizace.

Přesné klimatizační jednotky jsou navrženy tak, aby byl maximální poměr citelného chladicího výkonu (ten který opravdu snižuje teplotu) k chladicímu výkonu celkovému, ten zahrnuje i latentní chladicí výkon, tedy nežádoucí kondenzaci vodní páry, jinak řečeno odvlhčování. Čím vyšší je faktor citelného chladicího výkonu, tím se snižují náklady na provoz klimatizace. Přesné klimatizační jednotky mají při chlazení IT technologií větší účinnost, neboť pracují s menším rozdílem teplot nasávaného a vyfukovaného vzduchu a především omezují na minimum nežádoucí odvlhčování.



Obrázek 37: Poměr odvlhčení

Správně navržené přesné klimatizační jednotky jsou schopny udržet teplotu v místnosti s přesností $\pm 1^\circ\text{C}$ což je pro technologii daleko příznivější než větší kolísání teplot a vlhkosti způsobené komfortní klimatizací.



Obrázek 38: Poměr kolísání teplot

Přesné klimatizační jednotky pracují se zhruba trojnásobným průtokem vzduchu na srovnatelný chladicí výkon oproti jednotkám komfortním. Dokážou tedy daleko lépe zajistit optimální provětrání prostoru a zabrání vzniku tzv. hotspotů. Můžeme si je představit jako bubliny, kde je oproti zbylému vzduchu v místnosti mnohem tepleji. Ty pak mohou být příčinou lokálního přehřívání IT technologie.



Obrázek 39: Poměr průtoku vzduchu

Přesné klimatizační jednotky umožňují udržení stálé relativní vlhkosti vzduchu s přesností cca +/-5%. V případě potřeby je možno doplnit i zvlhčovač. Komfortní klimatizační jednotky oproti tomu snižují relativní vlhkost vzduchu, což může vést zejména v zimním období k poruchám IT technologie způsobeným statickou elektřinou.

Nejdůležitějším faktorem pro chlazení datových center je spolehlivost zařízení. Mějme na paměti, že přesné klimatizační jednotky jsou navrženy pro nepřetržitý provoz, tj. 24 hod x 365 dní v roce. Mohou pracovat v režimu chlazení i při venkovních teplotách -15 až -20°C. Oproti tomu u komfortních klimatizačních jednotek není naprostá spolehlivost nezbytná a tudíž, nebyla hlavním kritériem pro konstruktéra. Ten se řídil spíše náklady na výrobu, požadavkem na nízkou hlučnost a designem. Určitě nepředpokládal, že klimatizace bude v provozu i při venkovních teplotách hluboko pod bodem mrazu.

7.3.1.1 Požadavky na klimatizační zařízení

- 1) Chladicí výkon klimatizačního zařízení musí odpovídat celkové tepelné zátěži datového centra.
- 2) Operační rozsah venkovních teplot musí umožnit celoroční provoz v režimu chlazení tj. minimálně -15°C až $+40^{\circ}\text{C}$.
- 3) Musí být zvolen správný typ jednotky s ohledem na cirkulaci vzduchu v datovém centru, rozhodující je i její umístění.
- 4) Instalační možnosti zařízení – např. maximální délky potrubí a převýšení mezi vnitřní a venkovní jednotkou a hlukové parametry.

7.3.1.2 Určení chladicího výkonu

Chladicí výkon zařízení musí s rezervou cca 20% pokrýt celou tepelnou zátěž datového centra. Celková tepelná zátěž je součtem vnitřní tepelné zátěže (teplo vysálané z IT technologií) a vnějších tepelných zisků.

Vnitřní tepelná zátěž zhruba odpovídá součtu elektrických příkonů IT technologie (elektrický příkon se nakonec promění v teplo) a elektrických příkonů ostatních současně zapnutých spotřebičů (osvětlení, atd.). Ostatní zdroje tepla např. topení je nejlépe eliminovat.

Vnější tepelné zisky jsou závislé na tepelných vlastnostech budovy, velikosti, orientaci a zastíněním oken, umístěním datového centra v budově a dalšími faktory.

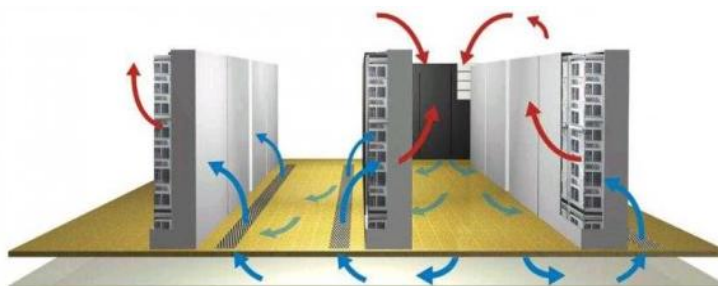
7.3.2 Návrh chlazení středních a velkých datových center

Při navrhování středních a velkých datových center se vychází z tepelné zátěže, kterou vyzáří IT technologie na m^2 (tab. 4).

Tabulka 4: Hustota tepelného zatížení

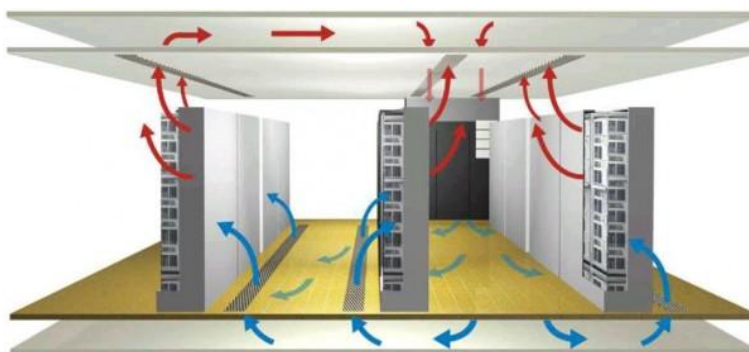
	Hustota zatížení (W/m^2)		
	Nízké	Střední	Vysoké
Společně umístěná zařízení, velká datová centra	< 1000	1000 – 1500	> 1500
Banky, finanční instituce, střední datová centra	< 600	600 – 1000	> 1000
Telekomunikační zařízení	< 500	500 – 750	> 750

Pro chlazení se používají téměř výhradně sálové klimatizační jednotky s distribucí vzduchu pod zdvojenou podlahu. Důležité je zvolit správnou minimální výšku zdvojené podlahy a důsledně dbát na rozmístění a orientaci rackových rozvaděčů systémem „studené“ a „teplé uličky“. Vzduch se přivádí distribučními elementy osazenými do podlahy prostoru „studené“ uličky a odsávání je u stropu „teplé uličky“.



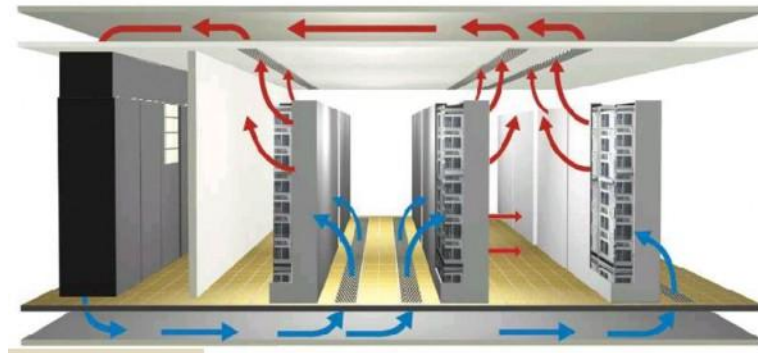
Obrázek 40: Teplá – studená ulička

Pro zvýšení účinnosti systému chlazení a umožnění větší intenzity tepelné zátěže je odtah vzduchu z „horkých“ uliček možno řešit zdvojeným stropem.



Obrázek 41: Zdvojený strop

Ještě vyšší bezpečnosti IT technologie a efektivity chlazení lze docílit oddělením prostoru klimatizačních jednotek od prostorů pro IT technologie.



Obrázek 42: Oddělení klimatizačních jednotek

Klimatizace velkých a středních datových center je v našich klimatických podmínkách vhodné doplnit o nepřímý freecooling. [23]

8 ZÁLOHOVÁNÍ

Je proces, při němž vzniká kopie zdrojových dat. Kopie zdrojových dat neboli datová záloha je obvykle uložena do jiného datového úložiště, než se nacházejí zdrojová data. Datová záloha může být komprimovaná nebo nekomprimovaná. V případě komprimované zálohy jsou obvykle záložní data uložena do souboru typu *zip*, *rar*, *tib* a další. Oproti archivaci dat, je při zálohování dat obvykle kladen důraz na možnost rychlé obnovy dat.

Zálohování dat se používá tehdy, když chceme data ochránit a v případě potřeby je obnovit v rozumném časovém intervalu. Jako příklad si představme účetní dokumenty, se kterými se pracuje každý den a přijít o ně by bylo nepříjemné. V takovém případě se vytvoří kopie takových dat a uloží se obvykle na jiném místě (např. NAS).[22]

Jak vyplývá z průzkumů, velké množství firem si pod pojmem záloha bohužel představuje, že stačí data jen zkopírovat do jiné složky na jejich počítači, případně serveru. Když se pak vyskytne problém, nezbyvá jim než vyhledat odbornou pomoc, která je mnohdy stojí několikrát víc, než investice do kvalitního zálohování.

8.1 Nejčastější příčiny ztráty dat

Protože dodnes nikdo nevymyslel jiný způsob, jak data spolehlivě ochránit před všemi typy hrozeb, patří zálohování k velice důležitým aspektům datové bezpečnosti. Dnes je dostupné velké množství programů určených na ochranu před viry a spyware, které jsou schopny naše data uchránit před vnějšími hrozbami. K Zabránění případné komunikaci mezi útočníkem a našim PC jsou dostupné softwarové i hardwarové firewally. Ale málokdo si dokáže uvědomit, že Faktorů, které ohrožují naše data, je víc než jen viry a jiné, jim podobné hrozby. Prostě možností jak přijít o data je mnohem více.[22]

8.1.1 Lidský faktor

Smazání, nebo přepsání dat vlastní vinnou je pravděpodobně jedna z nejčastějších příčin ztráty dat. V některých případech lze tuto ztrátu dat řešit za pomoci softwaru pro obnovu dat, ne vždy je však obnova dat úspěšná.

8.1.2 Selhání operačního systému

Řada uživatelů dělá jednu obrovskou chybu, neoddělují operační systém (ve zkratce OS) a data. Nevyužívají možnosti rozdělení disku na oddíly a ukládají tak svá data na systémový oddíl – tedy oddíl, na kterém je nainstalován OS. Ve chvíli, kdy dojde k selhání OS je tedy velmi pravděpodobná možnost ztráty dat uložených na systémovém oddílu. Pokud by stávající OS byl jen opraven, data zůstanou přesně tam, kde jsou. Ovšem oprava stávající instalace OS nemusí být vždy možná a nezbývá než volit novou instalaci, nebo obnovení tovární konfigurace. V těchto dvou případech s největší pravděpodobností přijdeme o všechna data.

8.1.3 Chyba aplikace

Na internetu je dnes volně ke stažení obrovské množství programů. Problém je ten, že nemůžeme tušit, jak se právě stažený program bude chovat, zda bude kompatibilní s OS, atd. Proto je dobré před každou instalací si ověřit, zda jde o nezávadný program. Pokud nemáme o funkcích programu a jeho fungování dostatek informací, je vhodné jeho instalaci odseparovat od ostatních programů a dat, vlastně vůbec od operačního systému. K tomu je ideální virtuální počítač (např. virtualbox).

8.1.4 Viry

Před touto hrozbou nás dostatečně kvalitně chrání antivirové, antispywarové programy, ale nemusí to být vždy pravda. Základem je mít tyto aplikace vždy aktualizované, ale i tak trvá někdy i několik hodin nebo dokonce dnů, než se objeví aktualizace pro nové hrozby. Společností zabývajících se zabezpečením systémů mají v dnešní době tendence integrovat antivirovou ochranu s možností vytvoření záloh do jediného softwarového balíčku.

8.1.5 Hardwarová porucha

I zde platí, že pokud nemáme zálohu, pak máme velký problém. Velikost problému pak záleží na typu hardwarové poruchy, ty lze rozdělit do dvou kategorií. Havárie pevného disku a havárie čehokoli jiného v PC. V prvním případě se jedná o skutečně velký problém, který bude stát pěknou sumu peněz. V tomto případě není jiné východisko než se

poohlédnout po firmách či programech určených na hardware data recovery. Ve druhém případě se dá říct, že o nic nejde, disk z poškozeného PC se zapojí do jiného funkčního PC a doufat, že data na disku jsou v pořádku. Problém může nastat tehdy, pokud jsou data na stejném diskovém oddílu jako operační systém. Některé operační systémy jsou na změnu hardwaru velice choulostivé. Pak se dostáváme k druhému případu a to selhání operačního systému.

8.1.6 Živelné pohromy

Přijít při požáru o fotky nebo videa z dovolené je pravděpodobně nepříjemné, ale nebude ten největší problém, který budou domácí uživatelé řešit. Firmy na tuhle skutečnost však nahlíží z úplně opačného pohledu na věc. Pokud pomineme drahé stroje a materiál, jsou pro firmy nejcennější informace a data. Většina firem má proto vlastní tzv. „disaster recovery“ plán, který jim v případě jakékoliv katastrofy, nejen živelné, umožní zprovoznit IT systémy a obnovit data. Kvalitní „disaster recovery“ plán počítá jednak s možností rychlé obnovy ze záloh, které jsou umístěny v místě firmy, ale i s možností obnovy díky zálohám, které jsou umístěny mimo společnost. [26]

8.2 Metody zálohování

8.2.1 Ruční zálohování dat

Nejjednodušší metoda zálohování, všichni ji známe a čas od času používáme. Metoda spočívá v tom, že se adresář určený k zálohování jednoduše zkopíruje do požadovaného úložiště. Výhoda je jasná hned na první pohled, jednoduchost. Nevýhodou je, že na takový způsob zálohování je nutné myslet a pamatovat. Pro zjednodušení této metody lze vytvořit jednoduchý dávkový soubor, který zkopíruje potřebná data do požadovaného úložiště.

8.2.2 Automatizované ruční zálohování dat

Jedná se v základě o stejnou metodu jako je ruční zálohování, jen s tím rozdílem, že ke spuštění dávkového souboru lze využít nástroje pro plánování úloh a celý proces tak automatizovat. Další alternativou, je využití volně dostupných programů (např. *Cobian*

Backup). Ty umožňují určit, co se má kam zálohovat a navíc umožňují i plánování zálohování.

8.2.3 Kopírování dat s komprimací

Opět v základu stejná metoda jako v předchozích dvou případech, jen kopírovaná data se komprimují. Komprimace neboli zhuštění dat, šetří místo potřebné pro ukládání záloh. Nevýhodou může být to, že pro to, abychom se dostali k záložním datům, která jsou komprimovaná, je musíme nejprve dekomprimovat. Za nástroje pro zálohování dat s komprimací, tak mohou být považovány například programy *WinZip*, *WinRAR*, atd., které umožňují kopírovaná data komprimovat ve výše zmiňovaných formátech (.zip, .rar, ...).

8.2.4 Automatizované zálohování dat s komprimací

Je ze skupiny metod založených na kopírování pravděpodobně nejdokonalejší. Zálohovaná data, jsou při kopírování do požadovaného úložiště komprimována a vše probíhá automaticky, bez jakéhokoliv podnětu uživatele. K této metodě lze za volně na internetu dostupné programy opět jmenovat *Cobian Backup*.

8.2.5 Vytváření obrazu

V případě zálohování větších celků je velmi pravděpodobné, že se setkáme s problémem, kterým je čas. Předchozí metody pracují tak, že načtou zdrojový soubor, který má být zálohován, zkomprimují tento soubor a uloží jej do potřebného umístění. Zálohovaný soubor se tedy musí nejdříve celý načíst, tím se značně prodlužuje čas, potřebný pro vytvoření zálohy. Pokud si tedy vezmeme 20 GB dat, které chceme zálohovat metodou kopírování dat na jiný lokální disk (přesun dat z lokálního disku na jiný lokální disk je nejrychlejší přenos) může tato operace trvat i několik hodin. Tenhle problém ale není neřešitelný.

Rychlejší metodou je vytváření obrazů diskového oddílu, tzv. image. Při této metodě se nepracuje s daty jako takovými, nýbrž s obsazenými sektory disku. Zjednodušeně lze říct, že k zálohovanému disku vytvoříme jeho identický klon. Díky tomu, že zálohované data se nemusejí načítat, je vytvoření zálohy mnohonásobně rychlejší. Aby toho nebylo málo, některé programy umožňují vybrat na diskovém oddílu jen konkrétní adresáře, tudíž není

potřeba zálohovat celý diskový oddíl o velikosti např. 300 GB, ale jen konkrétně to co je pro nás důležité.[26]

8.3 Typy záloh

8.3.1 Nestrukturovaná

Takovým typem záloh může být například větší množství CD/DVD disků s minimem informací o záloze. Jde o nejjednodušší typ zálohy, ale není vhodná pro větší objemy dat.

8.3.2 Úplná + Inkrementální

U tohoto typu záloh se vytváří více kopií zálohovaných dat. Jako první se vytvoří úplná záloha všech dat. Následně se přidávají jen ty soubory, u kterých došlo od poslední zálohy ke změně. Obrovskou nevýhodou tohoto typu záloh je, že v případě obnovení zálohy je nutné použít všechny zálohy od první úplné, až po zálohu, která je potřeba. To může být náročné na čas, ale hlavně takové zálohy zabírají poměrně dost místa.

8.3.3 Úplná + Rozdílová

Podobná jako inkrementální. Znovu se provede první úplná záloha. Pak se ukládají pouze nové nebo změněné soubory, nikoli od poslední zálohy, ale od té první úplné, i když některé už jsou obsaženy v předešlé částečné záloze. Obnova dat pak pracuje pouze s úplnou zálohou a poslední rozdílovou. [27]

8.3.4 Zrcadlová + Reverzně přírůstková

Používá se zde tzv. zrcadla, to zachycuje stav systému po poslední záloze a historii jednotlivých přírůstkových záloh. Každé zálohování se ihned promítne v zrcadle a soubory, u kterých došlo od poslední zálohy ke změně, jsou přesunuty do přírůstkové zálohy. Protože je potřeba pro každou zálohu mít možnost porovnání se zrcadlem, je tento typ záloh nevhodný pro přenosná media. Výhodou této zálohy je, že máme stále k dispozici aktuální plnou zálohu a ukládáme pouze historii změn.[26]

8.3.5 Úplná záloha systému

Záloha obsahuje kompletně celé PC včetně operačního systému – obraz disku (podkapitola – vytváření obrazu).

8.4 Zálohovací média

8.4.1 DVD disky

Nejrozšířenější a nejdéle používané médium pro zálohování je i dnes s oblibou používáno. K jednoznačným výhodám patří bezpochyby cena, která se postupně ustálila na přijatelné hranici. K nevýhodám patří odolnost proti fyzickému poškození, při neopatrném zacházení se životnost DVD disků rapidně snižuje.

8.4.2 Pevné disky

Teoreticky se dá říct, že se jedná o tentýž případ jako DVD disky, jen s výhodou několikanásobně větší kapacity. Pro disky staršího data vydání může být nevýhodou rozhraní (např. PATA rozhraní dnes nenajde podporu). Při volbě pevného disku jsou k dispozici dvě varianty, externí nebo interní. Využití interních disků je naprosto jasné, i když i přímo v počítači mohou sloužit k zálohování. Pro potřeby zálohování je však mnohem lepší volit externí disk. Ten je k PC připojen pomocí USB případně eSATA. To umožňuje značnou mobilitu, ale především možnost zapínat disk pouze v tu dobu, kdy jej opravdu potřebujeme pro zálohování.

8.4.3 Flash paměti

Používáme je snad všichni dnes a denně, USB „flashka“, nebo některá z mnoha paměťových karet (SD, micro SD, ...). I když jde o velice rozšířené médium, není pro potřeby zálohování příliš vhodné. Jejich největší slabinou je jejich konstrukce, ta umožňuje snadnou, náhlou a jednoduchou ztrátu dat. Pokud pomineme omezený počet zápisů, možnost zničení statickou elektřinou je nejčastější důvod ztráty dat ztráta samotného média. Ruku na srdce, komu se nikdy neztratila „flashka“? Další nevýhodou je cena za GB, ta se oproti běžným pevným diskům pohybuje mnohem výš.

8.4.4 NAS

Přenos dat probíhá pomocí TCP/IP nebo FTP protokolů, které jsou běžně používány k výměně dat na internetu. NAS je na rozdíl od externích pevných disků konstruován pro nepřetržitý provoz. Dalším rozdílem je možnost připojení několika PC současně. Systém je tak velice variabilní a NAS je mezi domácími uživateli, i přes vyšší cenu než externí pevný disk, stále oblíbenější.

8.4.5 Online zálohování

S poskytovateli online zálohování se v posledních pár letech roztrhl pytel. Je to pochopitelně dáno dostupností internetového připojení.

Tuto možnost nám poskytuje zpravidla třetí strana. Naše data zálohujeme jejich odesláním do úložiště poskytovatele. To s sebou ale nese i bezpečnostní rizika, protože naše data má v držení poskytovatel a nedůvěra z hlediska možnosti zneužití dat je určitě na místě. Pro tento způsob zálohování je také nutné mít opravdu kvalitní připojení k internetu a to zejména upload. [27]

II. PRAKTICKÁ ČÁST

9 NÁVRH ŘEŠENÍ AUTOMATICKÝCH ZÁLOH POMOCÍ TECHNOLOGIE NAS

Abychom mohli začít úspěšně zálohovat je nejprve nutná instalace a nastavení NAS serveru Fujitsu Celvin Q800. Po úspěšném nainstalování, nastavení a spuštění nového datového úložiště existují tři varianty řešení zálohování.

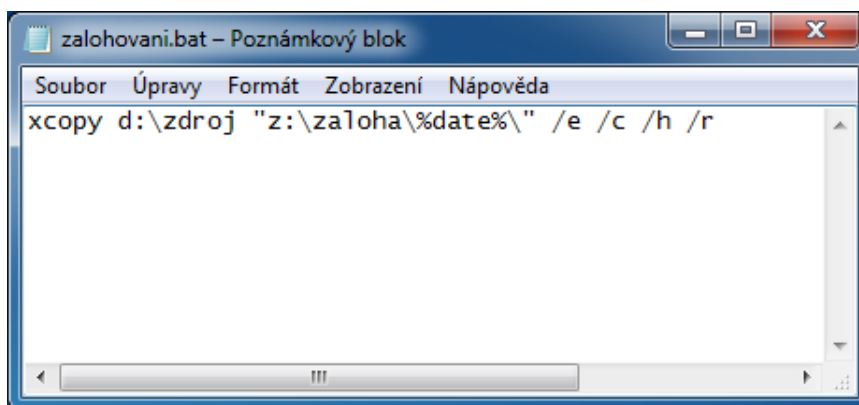
- 1) Ručně pomocí dávkového souboru a plánovače úloh, který je integrován v OS.
- 2) S použitím softwaru NetBak replicator dodávaného společně s NAS serverem Fujitsu Celvin Q800.
- 3) S použitím jiného placeného/neplaceného softwaru určeného k zálohování (např. již několikrát zmiňovaný Cobian Backup).

9.1 Dávkový soubor a plánovač úloh

Tato varianta je pouze pro uživatele, kteří ovládají příkazovou řádku. Ale i v jejich případě tato varianta není nejvhodnějším řešením.

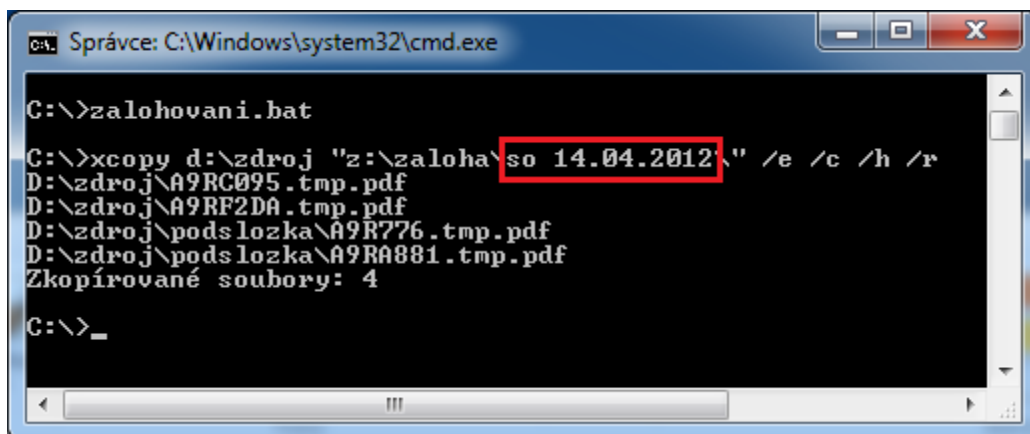
9.1.1 Vytvoření dávkového souboru

- 1) Otevřeme si poznámkový blok.
- 2) Napíšeme příkaz pro kopírování souborů.
 - Nejjednodušší je využití příkazu xcopy (obr. 43), pokud potřebujeme nakopírovat více adresářů, bude výsledný dávkový soubor obsahovat více řádků s podobným příkazem (měnit se bude jen zdrojový adresář, případně cílový).
- 3) Soubor uložíme s příponou .bat.



Obrázek 43: Ukázka kódu dávkového souboru

Tento dávkový soubor bude kopírovat vše co je obsaženo v adresáři „zdroj“ na NAS do adresáře „zaloha“ a podadresáře, který bude pojmenovaný dle data, ve kterém byla záloha spuštěna (obr. 44). To, že každá záloha bude ve své vlastní složce, eliminujeme problém, kdy se potřebujeme vrátit k některé předchozí verzi souboru, protože pokud bychom kopírovali do jediné složky, budeme mít k dispozici verzi souboru před poslední zálohou.



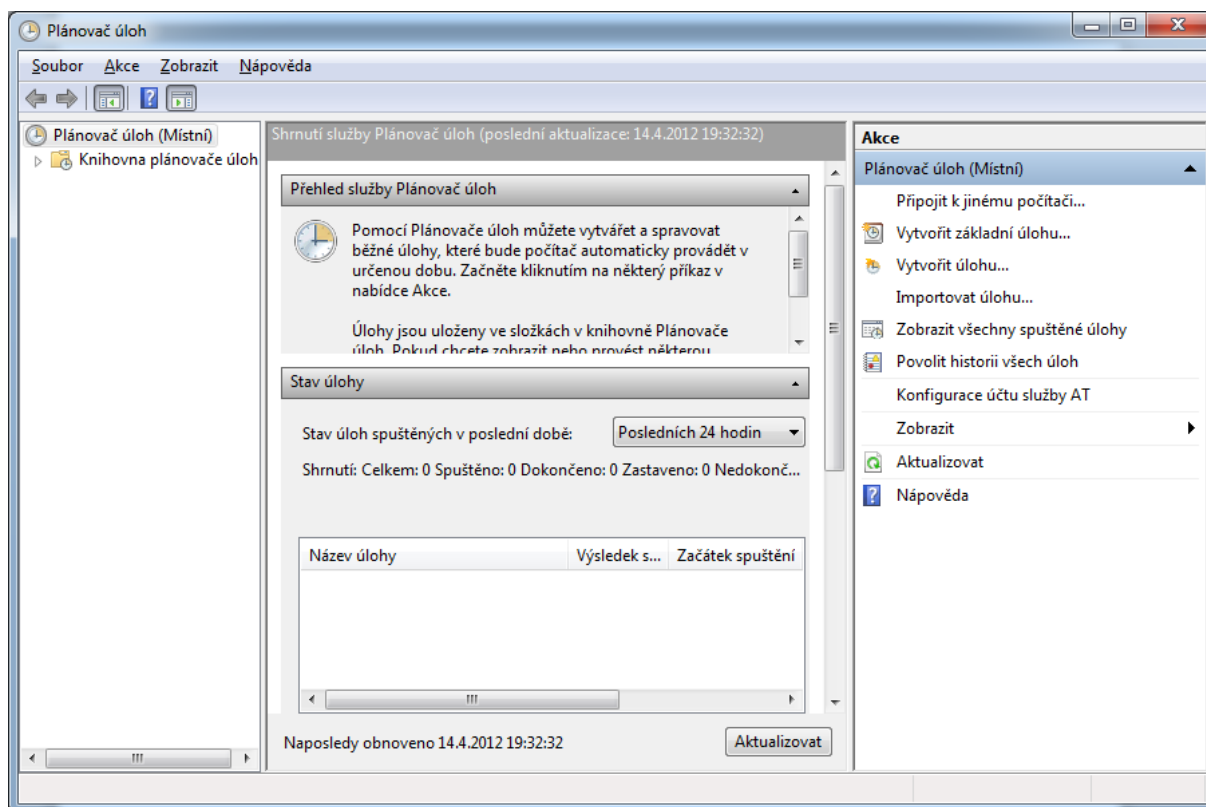
```
C:\Windows\system32\cmd.exe
C:\>\zalohovani.bat
C:\>\xcopy d:\zdroj "z:\zaloha\so 14.04.2012\" /e /c /h /r
D:\zdroj\A9RC095.tmp.pdf
D:\zdroj\A9RF2DA.tmp.pdf
D:\zdroj\podslozka\A9R776.tmp.pdf
D:\zdroj\podslozka\A9RA881.tmp.pdf
Zkopírované soubory: 4
C:\>\_
```

Obrázek 44: Výpis příkazové řádky po spuštění dávkového souboru


9.1.2 Vytvoření naplánované úlohy

1) Spustíme plánovač úloh (obr. 45)

- přes nabídku start
 - o Klikneme na tlačítko **Start**.
 - o Klikneme na položku Ovládací panely.
 - o Klikneme na položku Systém a údržba.
 - o Klikneme na položku Nástroje pro správu.
 - o Klikneme na nástroj Plánovač úloh.
- Pomocí příkazu „*taskschd.msc*“.



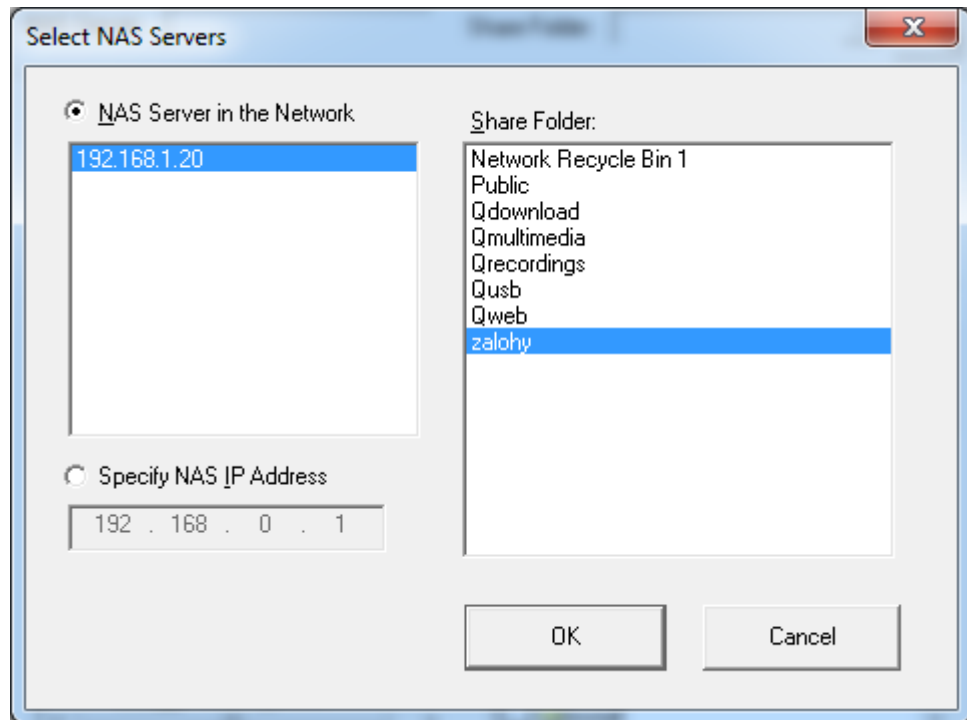
Obrázek 45: Základní zobrazení plánovače úloh – MS Windows 7

- 2) Klikneme na ikonku  „vytvořit základní úlohu“ - spustí se průvodce vytvořením základní úlohy.
- 3) V novém okně průvodce vyplníme pole „Název“, pole „Popis“ je nepovinné a můžeme jej nechat prázdné.
- 4) Vybereme, jak často má být úloha spouštěna – týdně.
- 5) Zvolíme dny v týdnu a čas, kdy se bude úloha spouštět – pondělí, středa, pátek ve 12:00, opakování každý týden – v poli „opakování“ ponecháme číslo 1.
- 6) Zvolíme požadovanou akci – spustit program.
- 7) Kliknutím na „procházet“ najdeme dávkový soubor „zalohovani.bat“
- 8) Při kliknutí na tlačítko dokončit se nám nová úloha uloží.

9.2 Fujitsu NetBak replicator

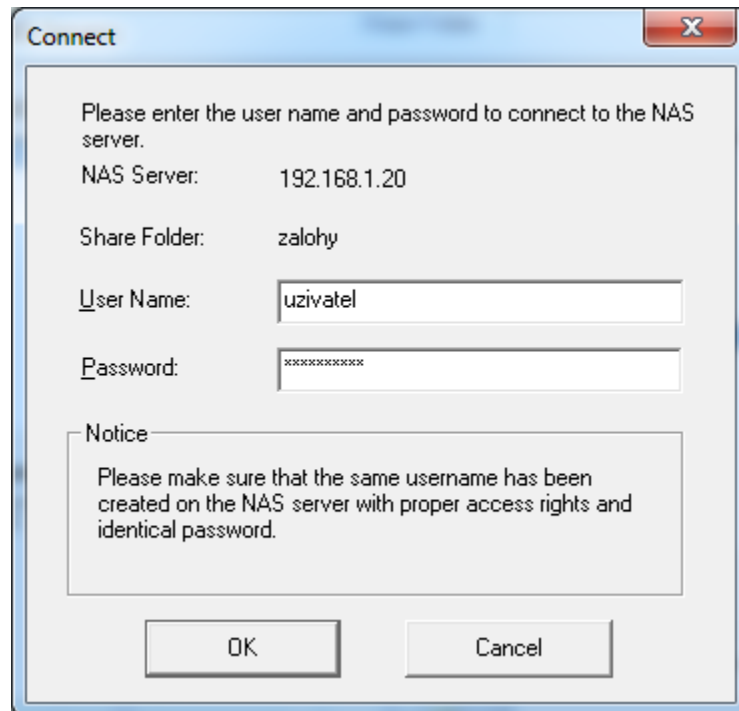
Software určený pro jednoduché a rychlé zálohování distribuovaný společně se zařízením řady Fujitsu NAS Calvin Q. Nevýhodou tohoto softwaru je absence české lokalizace, ovšem na jeho obhajobu je nutné říci, že jeho ovládání a nastavení automatických záloh je velmi rychlé a jednoduché.

Instalační soubor se nachází na přiloženém CD, „\Replicator\setup.exe“, nebo jej lze spustit pomocí autorun, kde vybereme „Install NetBak Replicator“. Po prvním spuštění nás program vyzve k vybrání NAS serveru a cílového adresáře pro naše zálohy (obr. 46)



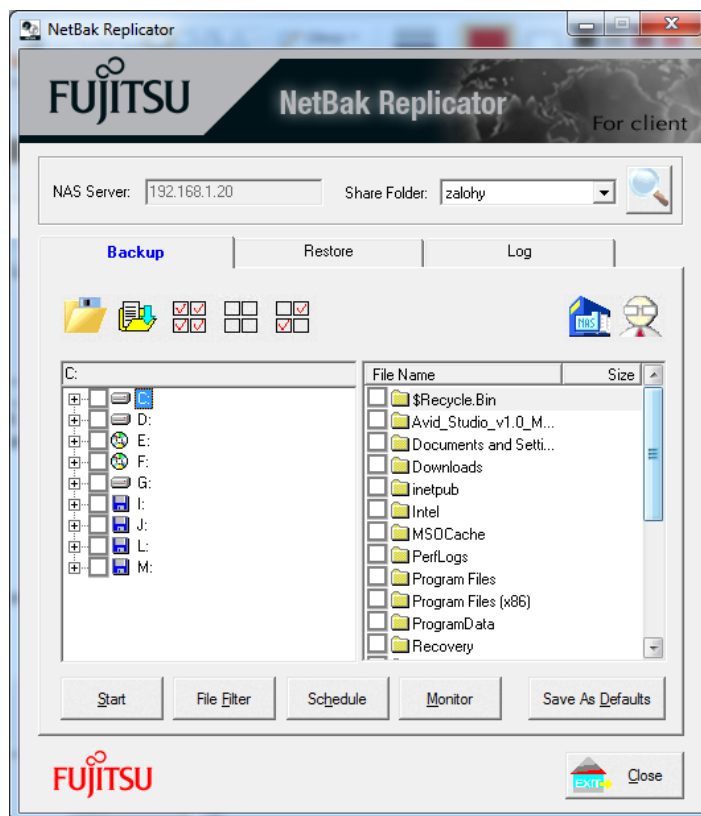
Obrázek 46: Základní nastavení NetBak Replicatoru

Po zvolení NAS serveru se objeví další dialogové okno, kde budeme vyzváni k zadání uživatelského jména a hesla pro přístup na NAS (obr. 47).



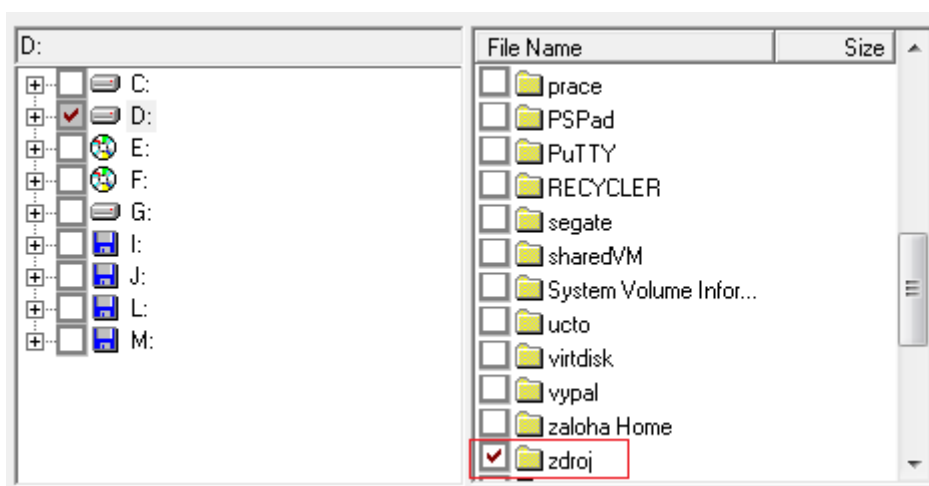
Obrázek 47: Připojení k NAS serveru

Pokud jsme zadali správné uživatelské jméno a heslo objeví se základní rozhraní (obr. 48). Nyní se můžeme směle vrhnout na nastavení automatických záloh.



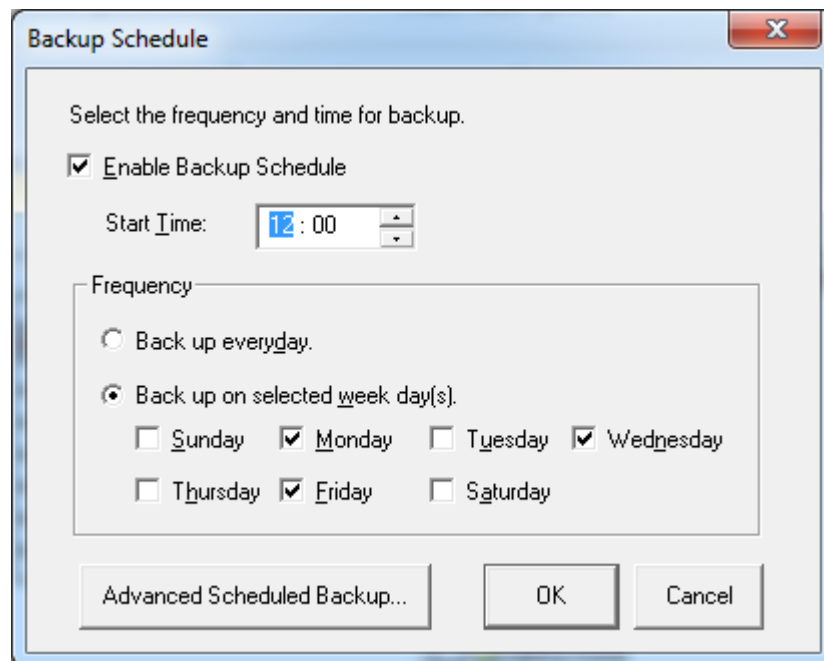
Obrázek 48: Základní rozhraní NetBak Replicatoru

- 1) Kliknutím na zaškrtačací políčko vybereme adresáře, které chceme zálohovat.
- v levém sloupci vybereme disk „D:“.
 - v pravém sloupci se zobrazí náhled adresářů a souborů zde umístěných.
 - kliknutím do prázdného čtverečku před názvem adresáře jej vybereme (obr. 49).



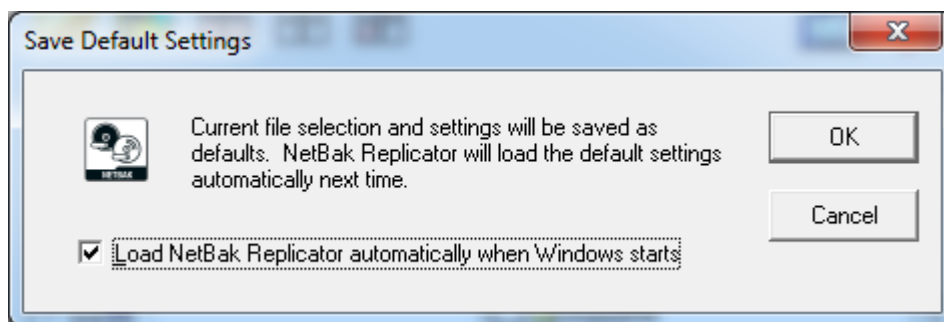
Obrázek 49: Označení adresářů k zálohování

- 2) Nastavíme, kdy se budou zálohy provádět.
- Klikneme na tlačítko „Schedule“.
- 3) V novém dialogovém okně nastavíme, kdy se budou automatické zálohy spouštět (obr 50).
- „Enable back up scheduled“ – aktivovat plánování záloh.
 - „Start time“ – čas kdy bude záloha spouštěna – 12:00.
 - „Back up on selected week day(s)“ – zálohovat ve zvolené dny v týdnu.
 - o Monday – pondělí
 - o Wednesday – středa
 - o Friday – pátek
 - Potvrdíme kliknutím na „OK“.



Obrázek 50: Nastavení rozvrhu zálohování

- 4) Uložíme nastavení kliknutím na „Save as defaults“. Objeví se nové dialogové okno, to jen potvrdíme stiknutím tlačítka „OK“ (obr 51). Vzápětí na to se objeví okno oznamující nám, že nastavení bylo uloženo.



Obrázek 51: Uložení nastavení

- 5) Klikneme na tlačítko „Monitor“, tím se provede první záloha, další zálohy poběží již podle nastaveného plánu.

Na závěr je nutné podotknout, že u této varianty, stejně jako u té předešlé dochází k pouhému kopírování souborů a adresářů. Jednotlivé rozdíly, výhody, nevýhody popisuje následující tabulka (tab. 5)

Tabulka 5: Porovnání zálohovacích metod


	Dávkový soubor + plánovač úloh	NetBak Replicator
Výhody	<ul style="list-style-type: none"> + Není potřeba specializovaný software (<i>možnost nastavení automatických záloh bez potřeby oprávnění uživatele k instalaci aplikací</i>). + K dispozici i předchozí verze souboru. 	<ul style="list-style-type: none"> + Jednoduchost (uživatelé pro nastavení zálohování stačí základní znalosti práce na PC). + Rychlost. + Oproti 1. variantě je potřeba méně místa pro zálohy.
Nevýhody	<ul style="list-style-type: none"> - Velikost záloh. - Znalost příkazové řádky. 	<ul style="list-style-type: none"> - K dispozici vždy jen verze souboru před poslední zálohou.

9.3 Cobian Backup

Výhodou této volby je téměř profesionální zálohování, které je volně dostupné všem díky freeware licenci. Krom toho, že je program volně ke stažení, je také kompletně v češtině, což mnohým značně usnadňuje jeho ovládání.

Po spuštění se může zdát, že jeho ovládání a nastavení bude problematické a komplikované, opak je ale pravdou.

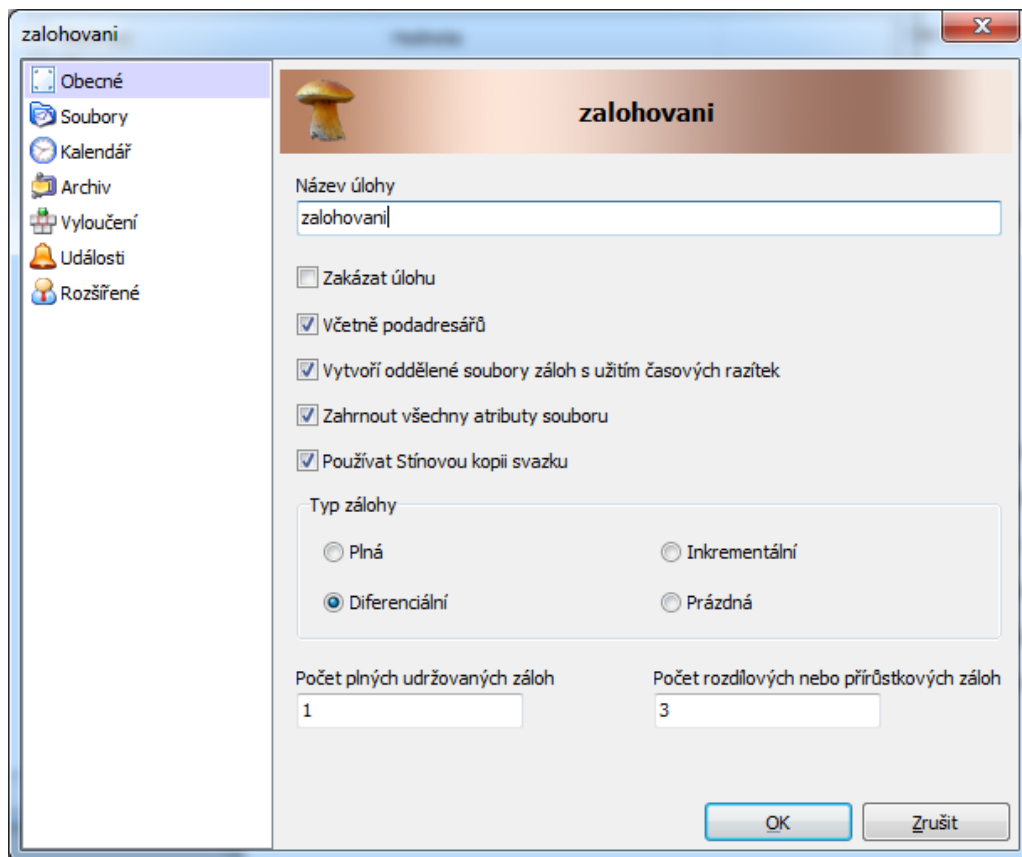


1) Kliknutím na ikonu  „Vytvořit novou úlohu“ se nám otevře nové okno, kde nastavíme parametry nové úlohy.

2) V obecných vlastnostech nastavíme parametry zálohování (obr 52).

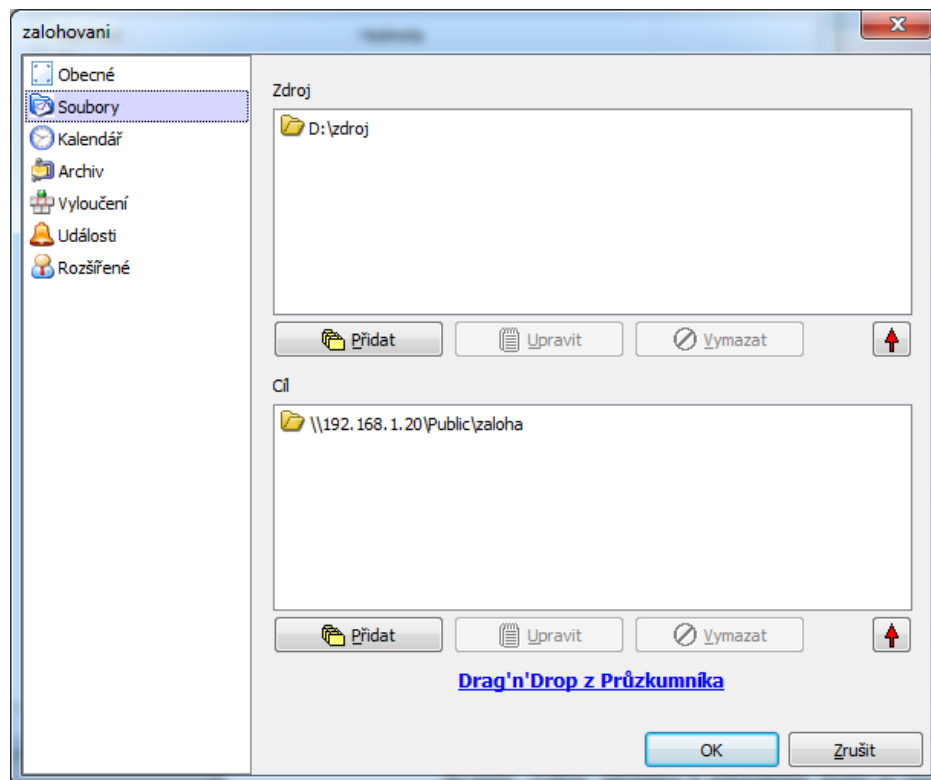
- včetně podadresářů
- vytvořit oddělené soubory záloh s užitím časových razítek
- zahrnout všechny atributy souboru
- používat stínovou kopii svazku
- typ zálohy
 - o diferenciální

- počet plných udržovaných záloh: 1
- počet rozdílových nebo přírůstkových záloh: 3



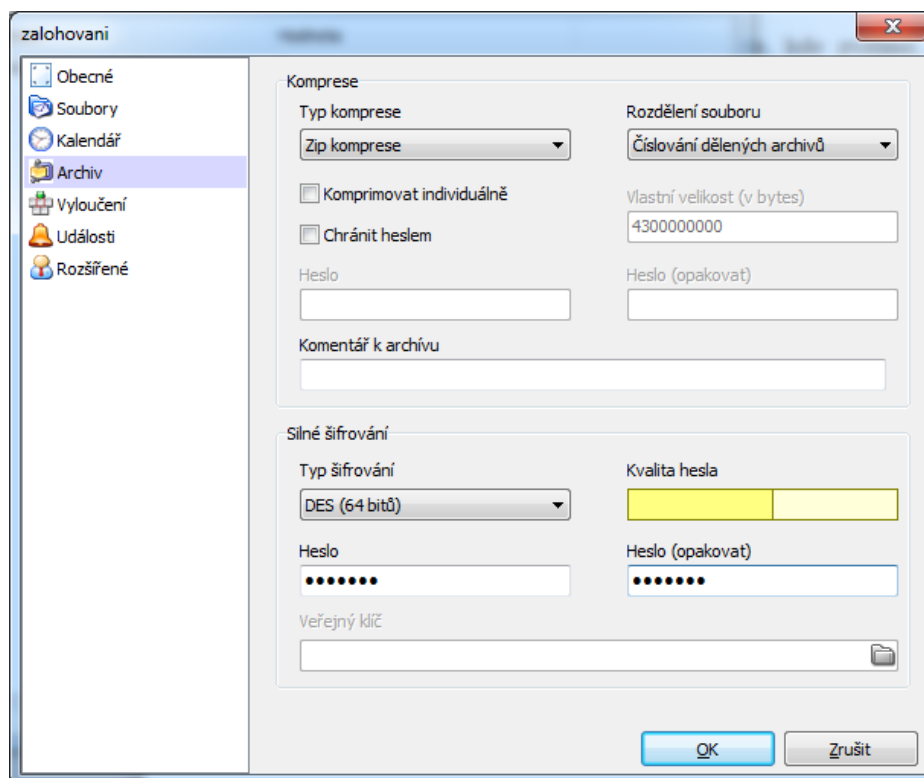
Obrázek 52: Obecné nastavení zálohování

- 3) Vybereme zdrojový adresář (případně zdrojové) a cílový. Můžeme zde využít funkce „Drag’n’drop“ – pomocí průzkumníka najdeme požadovaný adresář, ten přetažením do pole „Zdroj“ přidáme k adresářům, které se budou zálohovat.
- 4) Vybereme cílový adresář pro zálohy, opět můžeme využít funkce „Drag’n’drop“



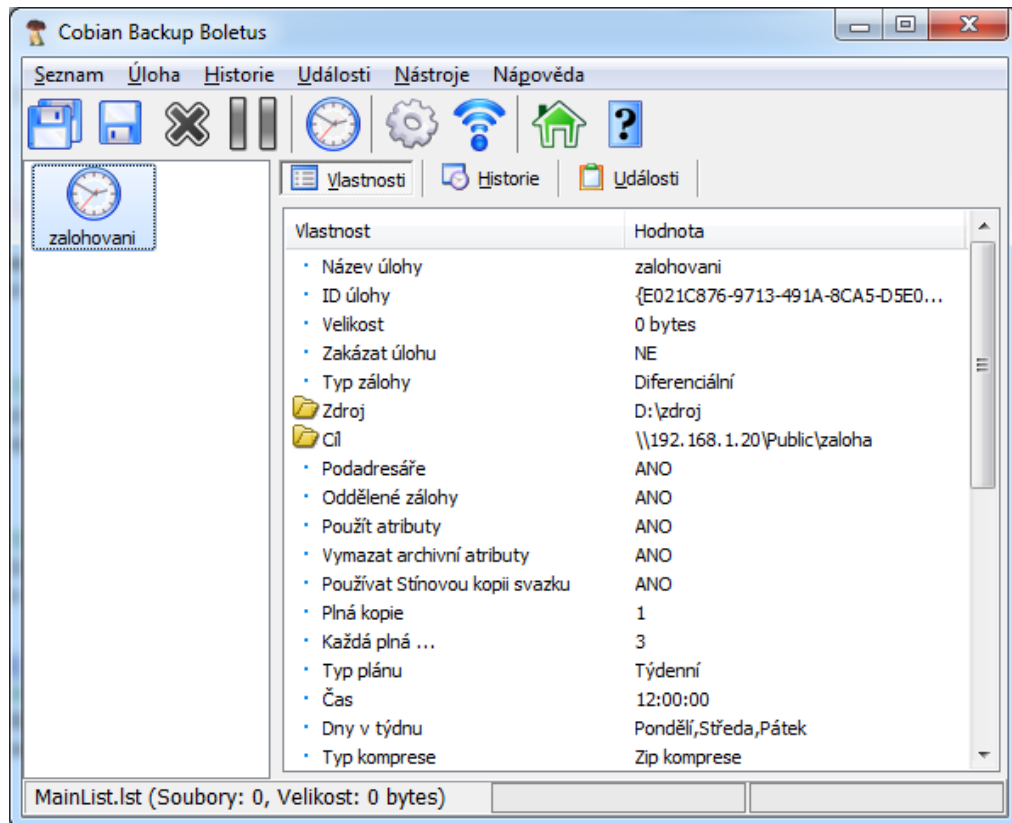
Obrázek 53: Nastavení zálohovaných adresářů a souborů

- 5) Dalším krokem je nastavení rozvrhu, kde zvolíme, jak často bude zálohování probíhat.
 - Typ plánu – týdenní
 - o pondělí, středa, pátek
 - čas zálohování – 12:00
- 6) V kroku archivace nastavíme, zda se budou zálohy komprimovat a zda budou chráněny heslem, nebo dokonce šifrovány.
 - metoda komprese zip
 - heslo není nutné vyplňovat
 - typ šifrování – DES
 - o heslo by mělo obsahovat velká a malá písmena, číslice a alespoň jeden speciální znak (@, &, %, ...), délka hesla by měla být větší jak 6 znaků
 - o kvalitu hesla nám graficky zobrazuje pole „kvalita hesla“ (obr. 54).
 - červená – slabé heslo
 - žlutá – průměrné heslo
 - zelená – silné heslo



Obrázek 54: Nastavení komprese a šifrování záloh

- 7) V tomto kroku je možné nastavit filtry pro soubory, které budou po splnění podmínek zálohovány, nebo naopak budou ze zálohy vyjmuty. Parametry mohou být jméno souboru, přípona, velikost, atributy, atd.
- 8) Záložka „Události“ slouží k nastavení operací, které se provedou vždy před spuštěním procesu zálohování, nebo po něm – není nutné nastavovat.
- 9) Posledním krokem v nastavení zálohování záložka „Rozšířené“ – není nutné nastavovat, pokud se úloha nebude spouštět pod jiným uživatelským účtem. V tom případě se musí vyplnit uživatelské jméno a heslo.
- 10) Potvrzením tlačítka „OK“ se nastavení uloží. Nově vytvořená úloha se objeví v levém sloupci s ikonou hodin, pokud na ni klikneme, v pravém sloupci se objeví parametry jejího nastavení (obr. 55).



Obrázek 55: Přehled vlastností zvolené úlohy

10 NÁVRH ZABEZPEČENÍ DATOVÉHO CENTRA

10.1 Údaje o klientovi

Rainbow meadia, s.r.o.

U Tescomy č.p. 254

760 01 Zlín, Lužkovice

IČO: 27276011

DIČ: CZ27276011

tel. +420 577 111 250

mob. +420 725 055 250

info@rainbow-media.cz

<http://www.rainbow-media.cz>

druh činnosti: reklamní agentura, server hosting, webhosting

10.2 Údaje o střežených objektech

10.2.1 Základní údaje

Adresa:

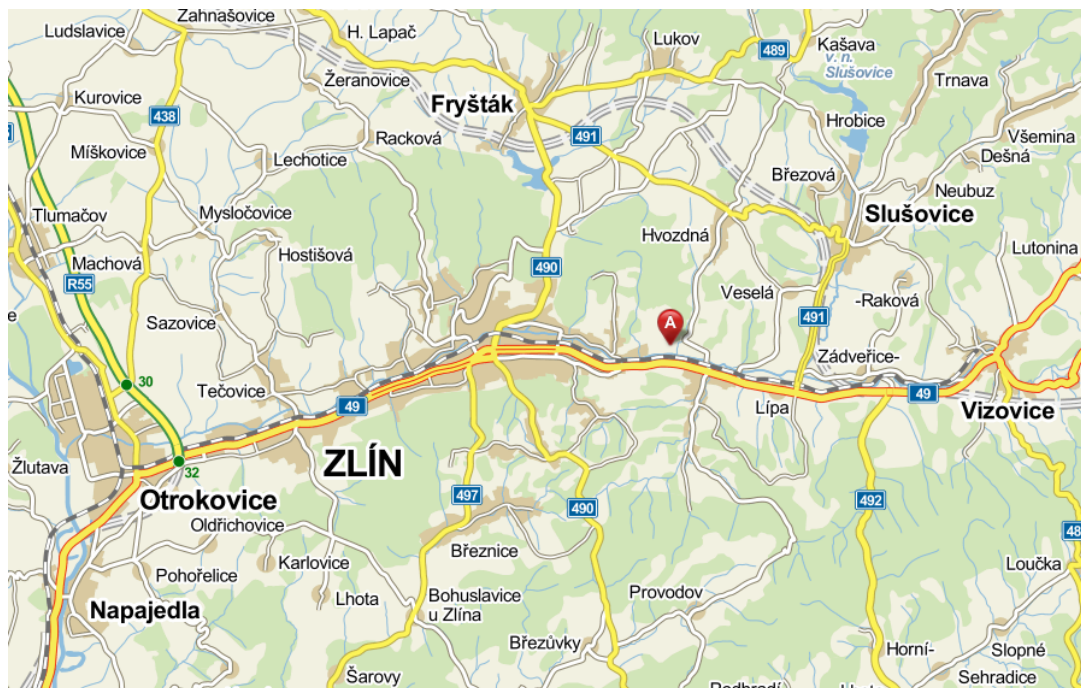
U Tescomy č.p. 254

760 01 Zlín, Lužkovice

Kontaktní osoba:

Ing. František Čížek

tel. 604 555 285



Obrázek 56: Poloha objektu

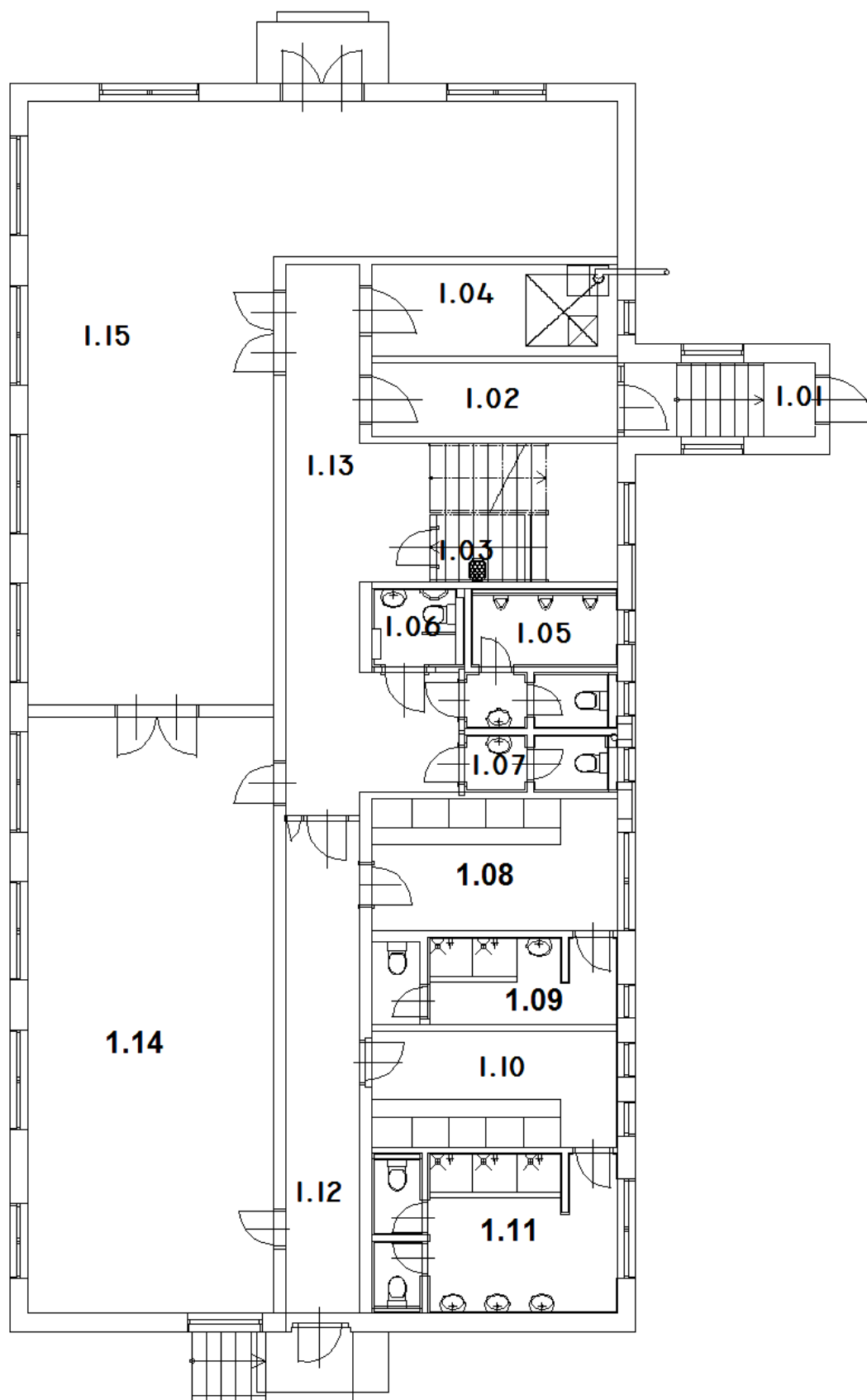
Popis:

Objekt představuje dvoupatrovou průmyslovou budovu situovanou na konci průmyslové zóny Zlín Příluky. V blízkém okolí se kromě dalších průmyslových budov nachází zahrádkářská kolonie.

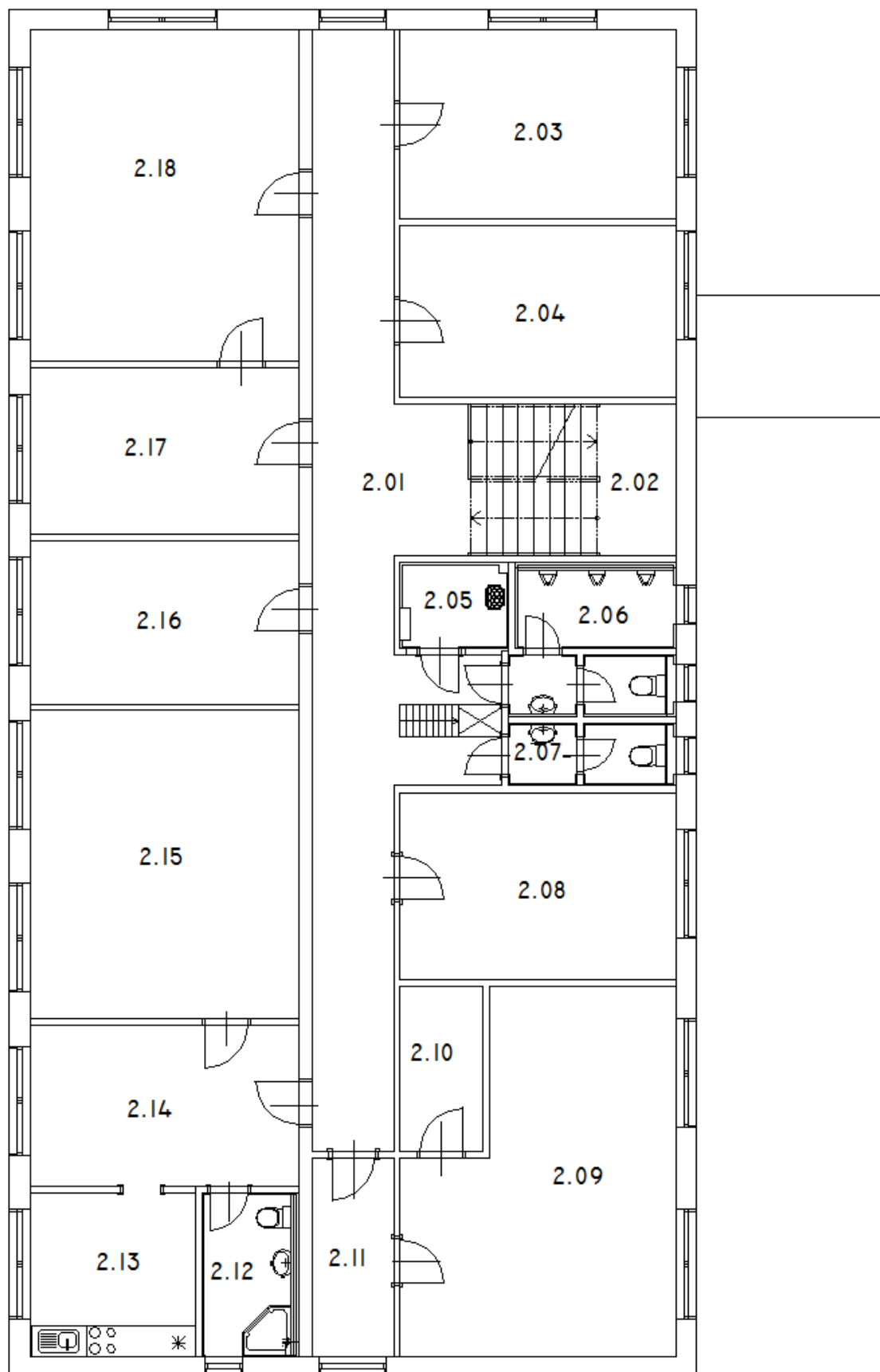


Obrázek 57: Letecký snímek okolí objektu

10.2.2 Půdorys objektu



Obrázek 58: Půdorys 1NP



Obrázek 59: Půdorys 2NP

10.2.3 Rozpis místností a třída prostředí

Tabulka 6: První poschodí

č. místnosti	popis	třída prostředí
1.01	zádveří	II
1.02	vstupní chodba	II
1.03	úklidová místnost	II
1.04	technická místnost	II
1.05	toalety – muži	II
1.06	toalety – ženy	II
1.07	toalety – invalidé	II
1.08	šatna – ženy	II
1.09	sprcha – ženy	II
1.10	šatna – muži	II
1.11	sprcha – muži	II
1.12	chodba	II
1.13	chodba	II
1.14	tiskárna	II
1.15	sklad + expedice	II

Tabulka 7: Druhé poschodí

č. místnosti	popis	třída prostředí
2.01	chodba	II
2.02	meziposchodí	II
2.03	jednací místnost	I
2.04	místnost pro návštěvy	I
2.05	úklidová místnost	II
2.06	toalety – muži	II
2.07	toalety- ženy	II
2.08	kancelář	I
2.09	datové centrum	II
2.10	místnost pro SHZ	I
2.11	vstupní místnost pro datové centrum	II
2.12	hygienické zařízení	II
2.13	denní místnost	I
2.14	kancelář asistentky	I
2.15	kancelář ředitele	I
2.16	kancelář	I
2.17	kancelář hlavního grafika	I
2.18	grafické centrum	I

10.3 Stupeň zabezpečení

Tabulka 8: Stanovení stupně zabezpečení

Zabezpečuje se	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
okna		O	O+P	O+P
vstupní dveře	O	O	O+P	O+P
ostatní otvory		O	O+P	O+P
stěny			P	P
stropy, střechy			P	P
podlahy				P
prostor místností	T	T	T	T
objekt (vysoké riziko)			S	S
<p>vysvětlivky: O – otevření P – průnik T – past S – objekty se speciální pozorností</p>				

10.4 Přehled zařízení

1) PIR detektor s připojením na sběrnici

- s plně digitálním zpracováním signálu. Detektor se připojuje přímo na sběrnici a komunikuje obousměrně s ústřednou DIGIPLEX EVO.

2) Magnetický kontakt

- Připojený na čtyř drátovou sběrnici, po které komunikuje přímo s ústřednou DIGIPLEX EVO. Je určený k povrchové instalaci

3) Vnitřní siréna

- vnitřní piezosiréna vybavená i optickou signalizací.

4) Venkovní siréna

- venkovní zálohovaná siréna s akustickou a optickou signalizací. Použitím mikroprocesoru v siréně lze vyhodnocovat nabití akumulátoru, vstup SERVICE eliminuje akustickou signalizaci. Sirénu lze aktivovat odpojením

napájecího napětí nebo přivedením střídavého napětí, rovněž je možné nastavit samostatnou aktivaci blikáče. Vnitřní plechový kryt zvyšuje odolnost sirény proti mechanickému poškození.

5) Detektor plynu – CO

- vyhodnocuje přítomnost nebezpečného jedovatého oxidu uhelnatého (CO) ve střeženém prostředí.

6) Detektor plynu – zemní plyn

- vyhodnocuje množství výbušného plynu (zemní plyn) ve střeženém prostředí, pomocí měření v ionizační komůrce a při výskytu méně než 1 množství LEL (lower explosive limit – mezní spodní hranice výbušné směsi) vyhlásí poplach.

7) Komunikátor

- univerzální IP/GPRS komunikátor, umožňující posílat poplachové zprávy na PCO přes internet nebo přes mobilní síť. Má konektor RJ45 pro připojení do sítě. Modul s GPRS může sloužit i pro přenos SMS zpráv.

8) Ústředna

- vhodná pro střední a velké objekty s možností instalace rozsáhlejší sběrnice. Počet podsystémů 4/8, počet zón 48/192, nastavba přístupu ACCESS. Jde o plně adresovatelný sběrniceový systém, do kterého lze zařadit až 127/254 sběrniceových modulů (klávesnice, bezdrátová nastavba, expandery, PGM výstupy, doplňkové zdroje, posilovače sběrnice, komunikační moduly IP, GSM, GPRS, ...), i samostatné sběrniceové detektory.

9) Akumulátor

10) Elektromechanický zámek

- Elektromechanický zámek, který propouští přes horní západku běžného kování a montuje se do zárubně nebo nepohyblivé části dvoukřídlých dveří.

11) Videotelefon

12) Docházkový terminál

13) Přístupový terminál

14) Čtečka otisku prstů a karet

15) Modul pro ACS

- Nadstavbový modul určený k připojení čteček karet a otisků prstů k ústředně DIXIPIX EVO.

16) Licence pro SW přístupového systému VAR-NET

- Licence dovoluje evidenci až 50 uživatelů (zaměstnanců), možnost rozšíření licence na 100 respektive 200 uživatelů.

17) IP kamera

- Barevná IP box kamera pracující v režimu den / noc (mechanický IR filtr), je určena pro vnitřní aplikace. Kamera nabízí volitelnou kompresi H.264/MPEG4/MJPEG, dual streaming, 1 megapixelové rozlišení (1280 x 800) s frekvencí až 15 snímků/s a automatické řízení clony.

18) NAS server

- *Fujitsu Celvin Q800* s kapacitou 8 TB (4x 2 TB), podpora RAID 0/1/5/6, vhodný pro malé a střední firmy. Zálohování, sdílení, kamerový systém, ...

10.5 Konfigurace systému

Systém bude rozdělen na 3 podsystémy:

- 1) První patro – možné odstřežit z klávesnice u vchodu.
- 2) Druhé patro – možné odstřežit z klávesnice u vchodu.
- 3) datové centrum – trvale zastřežen, lze jej odstřežit jen otiskem prstu pověřené osoby, při odchodu z datového centra opět otiskem prstu uveden do zastřeženého stavu.

Každý uživatel z celkového počtu 37, bude zařazen do skupiny podle přístupových oprávnění.

- 1) První skupina (dělníci, skladníci) – svým kódem odstřeží **podsystém 1**.
- 2) Druhá skupina (grafici, technici, zaměstnanci v kancelářích) – svým kódem odstřeží podsystém 1 a 2.
- 3) Třetí skupina (ředitel, pověřené osoby) – svým kódem odstřeží **podsystém 1 a 2**, po ověření pověřené osoby kontrolou otisku prstu odstřeží **podsystém 3**.

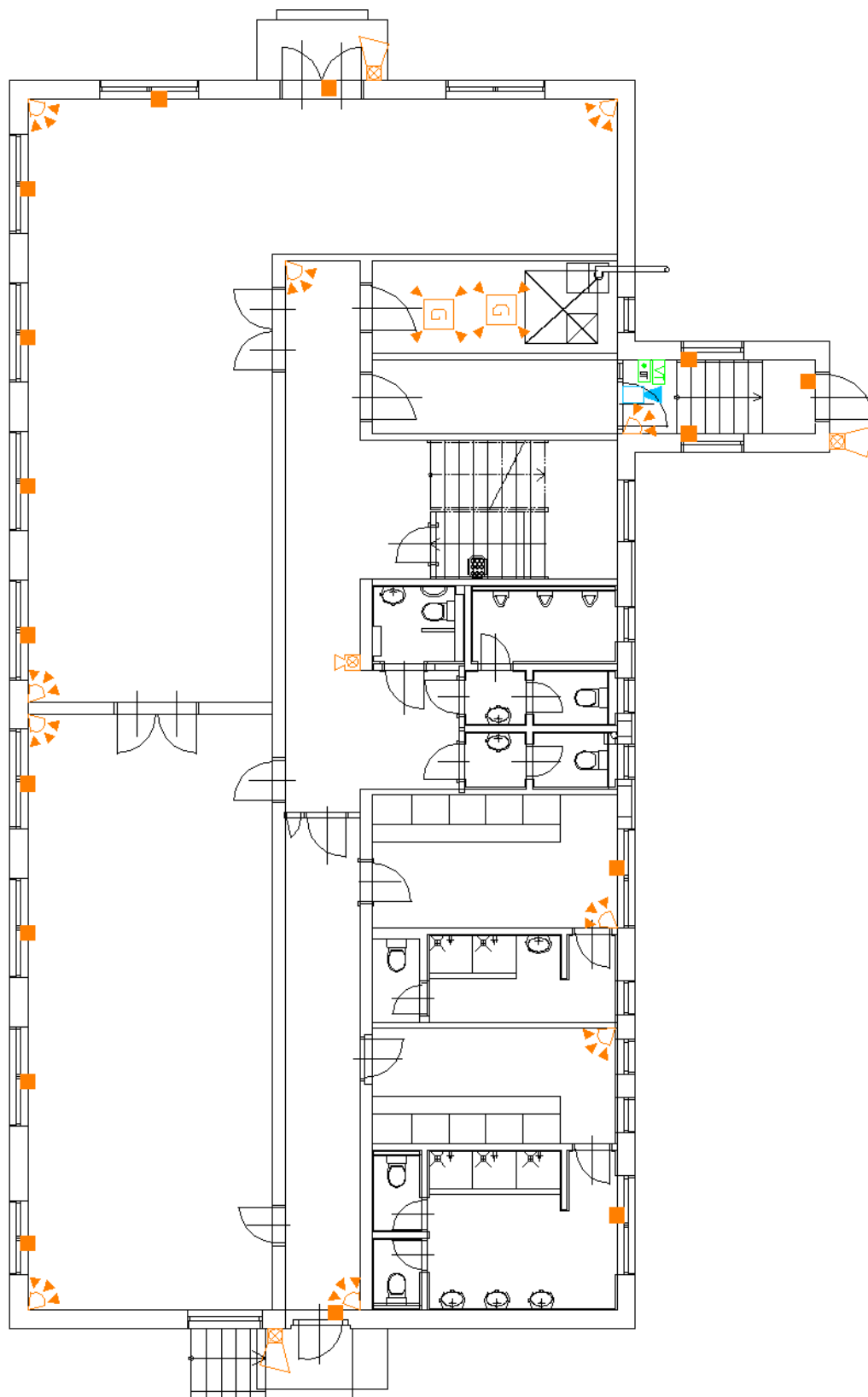
Po přijetí poplachového signálu při narušení podsystému 1 bude nejprve kontaktována pověřená osoba, v případě narušení v podsystému 2 nebo 3, bude tato skutečnost zkontrolována do 15 minut výjezdovou skupinou. Doba aktivace sirény je 15 minut – doba do příjezdu výjezdové skupiny.

10.5.1 Rozdělení do zón

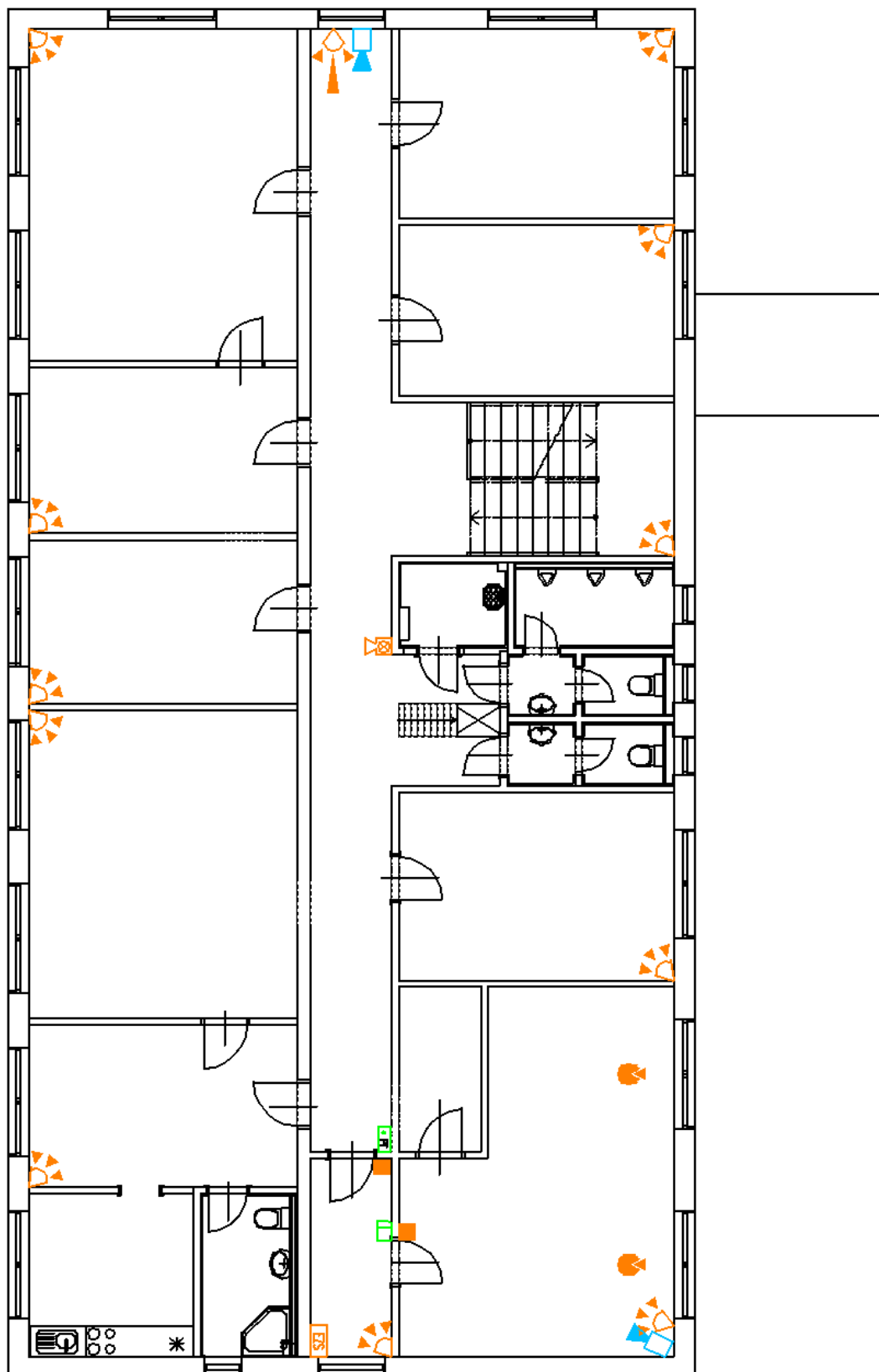
Tabulka 9: Přehled zón

č. zóny	č. místnosti (popis)	Typ zóny
1	1.01 hlavní vchod – otevření + PIR	zpožděná 30s
2	1.08 okno – otevření	okamžitá
3	1.09 okno – otevření	okamžitá
4	1.12 dveře (únikový východ) - otevření	okamžitá
5	1.14 okna -otevření	okamžitá
6	1.15 okna – otevření	okamžitá
7	1.15 dveře (východ) – otevření	okamžitá
8	1.01 okna – otevření	okamžitá
9	1.12 + 1.13 – PIR	okamžitá
10	1.08 – PIR	okamžitá
11	1.10 – PIR	okamžitá
12	1.14 – PIR	okamžitá
13	1.15 – PIR	okamžitá
14	1.04 – detektory plynu	okamžitá
15	2.02 – PIR	okamžitá
16	2.03 – PIR	okamžitá
17	2.04 – PIR	okamžitá
18	2.08 – PIR	okamžitá
19	2.09 dveře – otevření	okamžitá
20	2.09 okna – otevření	okamžitá
21	2.09 okna – průnik (rozbití)	okamžitá
22	2.11 dveře -otevření	okamžitá
23	2.11 – PIR	okamžitá
24	2.14 – PIR	okamžitá
25	2.15 – PIR	okamžitá
26	2.16 – PIR	okamžitá
27	2.17 – PIR	okamžitá
28	2.18 – PIR	okamžitá
29	2.01 – PIR	okamžitá

10.5.2 Rozmístění prvků



Obrázek 60: Rozmístění prvků 1NP



Obrázek 61: Rozmístění prvků 2NP

Poznámka: seznam použitých symbolů a podrobné výkresy jsou umístěny v příloze

10.6 Hlášení poplachu

Hlášení poplachu je řešeno pomocí GSM/IP modulu připojeného k ústředně. Ten odesílá signál do poplachového přijímacího centra (PPC) – dříve pult centralizované ochrany (PCO), a formou SMS na zvolená telefonní čísla.

Připojení k PPC bude realizováno firmou SYSTEM PLUS, s.r.o. s provozovnou ve Zlíně na adrese: ul. Pod Babou 4260, Zlín 760 01.

10.7 Normy a legislativa

Zákon č. 22/1997 Sb. – O technických požadavcích na výrobky.

Nařízení vlády č. 17/2003 Sb. – Základní technické požadavky na elektrická zařízení nízkého napětí.

Nařízení vlády č. 616/2006 Sb. – Základní technické požadavky na výrobky z hlediska jejich elektromagnetické kompatibility.

Skupina norem **ČSN EN 50 131** – Poplachové zabezpečovací a tísňové systémy.

Dále vybrané normy ze skupiny norem:

ČSN EN 50 132 – Kamerové sledovací systémy

ČSN EN 50 133 – Systémy kontroly vstupu

10.8 Certifikáty

Všechny použité prvky systému splňují požadavky pro daný stupeň zabezpečení a jsou k nim vydány certifikáty příslušnými úřady. Jednotlivé certifikáty jsou přiloženy v příloze.

10.9 Zásah

Zásah bude prováděn zásahovou jednotkou firmy SYSTEM PLUS, s.r.o. Dojezdová vzdálenost od provozovny je 7,1 km, předpokládaná doba dojezdu je 10-15 minut od vyhlášení poplachu. Dojezdová doba Policie České Republiky je do 10 minut od ohlášení.

10.10 Údržba a opravy

Správa, údržba a opravy systému budou prováděny firmou SYSTEM PLUS, s.r.o.

ZÁVĚR

Vzhledem k tendenci dnešní doby, kterou je centralizace systémů a s tím spojené shromažďování dat, které jsou mnohdy pro existenci firmy naprosto zásadní, na jednom místě roste i míra rizika ztráty těchto dat. Proto je nutné věnovat zabezpečení datového centra patřičnou pozornost. Nestačí zaměřit se na jednu konkrétní bezpečnost, nýbrž na jejich vzájemné propojení, počínaje personální a fyzickou bezpečností konče. Skutečnost je však úplně jiná a do zabezpečení především malých firemních datových center se příliš neinvestuje. Ovšem jen do té doby, než se nevyskytne nějaký problém, jehož vyřešení je mnohdy nákladnější, než investice do řádného zabezpečení datového centra.

Při zabezpečování datového centra je vhodné začít již u distribuce elektrické energie, která je pro datové centrum důležitá. Pokud se jedná o menší datové centrum, postačí instalace jednoduchých off-line, případně line-interactive UPS jednotek. Pro střední a velká datová centra je pak vhodné mít navíc i náhradní nezávislý zdroj energie např. v podobě dieselaagregátu.

Další nesmírně důležité pro správný a bezporuchový provoz je chlazení, které není dobré podceňovat, protože při přehřívání IT zařízení se rapidně snižuje jejich životnost a spolehlivost.

Bezesporu k zabezpečení datového centra patří i poplachové systémy stejně jako mechanické zabezpečení, které je vhodné doplnit i o kontrolu vstupu, čímž se zajistí, že do datového centra budou mít přístup pouze osoby pověřené a především ověřené. Pro malé datové centrum je možnost instalace autonomních systémů, jejichž pořizovací náklady jsou přijatelné i pro malé firmy.

V neposlední řadě je nutné myslet na protipožární opatření, která hrají svou roli především u středních a velkých datových center a instalace SHZ je naprostou samozřejmostí. V případě malých datových center je potřeba zvážit veškerá rizika a náklady spojené s instalací SHZ.

Vše je vhodné doplnit ještě o kvalitní monitoring, ať už se jedná o kamerový systém, monitorování klimatizace, či provozu samotných IT zařízení.

CONCLUSION

Current trend is the centralization of systems and related data collection in one place. In many cases the data is important for companies and their existence. Therefore we must pay attention to protect data center. It is not enough to focus on one particular protection but we must focus on their connections. It is begin from personnel protection and over whit physical protection. But the reality is completely different and companies do not want invest too much to protection especially for small corporate data centers. But until just before the problems occur which solution are often more expensive than investing in better protection of data center.

In data center protection we must begin from distribution of electric energy which is very important for data center. If it is a small data center simply enough to install off-line or line-interactive UPS units. For medium or large data centers is also advisable to have an independent and alternative energy sources such as diesel generator.

Another extremely important for the proper and correct operation is cooling which is not good to underestimate because overheating IT equipment rapidly reduces their service life and reliability.

To protection of the data center include alarm systems as well as mechanical protection. All of that are should be supplemented by access control system, ensuring that to the data center will have access only authorized and especially verified persons. For small data center is an installation option of autonomous systems. The costs of these systems are acceptable for small companies.

Finally, we must not forget the fire protection which is important in medium and large data centers. Of course, the installation of sprinkler system is necessary. In the case of small data centers need to consider all the risks and costs associated with the installation of sprinkler system.

All of this is suitable to add a quality monitoring, such as a camera system, monitoring air conditioning, or monitoring of IT, etc.

SEZNAM POUŽITÉ LITERATURY

- [1] HEJTMÁNEK, Ondřej. *OPTICKÉ KABELY V MODERNÍCH DATOVÝCH CENTRECH*. Brno, 2010. Bakalářská práce. Vysoké učení technické v Brně.
- [2] TIA-942. *Telecommunications Infrastructure Standard for Data Centers*. Arlington, VA: TELECOMMUNICATIONS INDUSTRY ASSOCIATION, 2005.
- [3] XANADU a.s. [online]. © 2012 [cit. 2012-04-29]. Dostupné z: <http://www.xanadu.cz>
- [4] Apex Microsystems: Solution. *Apex Microsystems* [online]. © 2009 [cit. 2012-04-29]. Dostupné z: http://www.apexmicrosystems.com/?page_id=518
- [5] KRÁLÍK, Lukáš, Lukáš FEHÉR, et al. *Metodika návrhu MZS*. Zlín, 2009. Seminární práce. Univerzita Tomáše Bati ve Zlíně.
- [6] IVANKA, Ján. *Mechanické zábranné systémy*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. ISBN 978-80-7318-910-5.
- [7] Zabezpečení dveří proti krádeži. *Policie České Republiky* [online]. © 2010 [cit. 2012-04-02]. Dostupné z: <http://www.policie.cz/clanek/zabezpeceni-dveri-proti-kradezi.aspx>
- [8] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. S.l.: Cricetus, 2006, 351 s. ISBN 80-902-9382-4.
- [9] COMPLETE CZ, spol. s.r.o. [online]. © 2011 [cit. 2012-04-02]. Dostupné z: <http://www.completecz.cz/>
- [10] ČEN EN 50131-1. *Poplachové zabezpečovací a tishňové systémy: systémové požadavky*. Praha: Český normalizační institut, 2007.
- [11] UHLÁŘ, Jan. *Technická ochrana objektů. II. díl: Elektrické zabezpečovací systémy II*. Praha: Policejní akademie české republiky, 2005. ISBN 80-7251-189-0.
- [12] JABLOTRON ALARMS A.S. *Jablotron* [online]. © 2008 - 2012 [cit. 2012-04-29]. Dostupné z: <http://www.jablotron.cz>
- [13] Přístupový systém. *ID karta: identifikační systémy* [online]. © 2012 [cit. 2012-05-01]. Dostupné z: <http://www.id-karta.cz/aplikace-1/pristupy-a-vstupy-5/>

- [14] Docházkové systémy: Tetronik. *RM KOM* [online]. (c) 2000 - 2012 [cit. 2012-05-01]. Dostupné z: <http://www.rm-kom.cz/index.php?link=zabezpecovaci-technika-katalog&hlavnikategorieid=2&vyrobceid=13&kategorieid=13>
- [15] Systémy kontroly vstupu. *Alarmtechnik Praha* [online]. 2007 [cit. 2012-05-01]. Dostupné z: <http://www.alarmtechnik.cz/systemy-kontroly-vstupu-acces.htm>
- [16] *Kvapilik: požární ochrana* [online]. © 2009 [cit. 2012-04-29]. Dostupné z: <http://www.kvapilik.net>
- [17] EPS Esser. *Colsys* [online]. 2006, 2.11.2010 [cit. 2012-04-29]. Dostupné z: <http://www.colsys.cz/cz-05weak-eps-esser.php>
- [18] HOŠEK, Zdeněk. Autonomní hlásiče kouře. In: *TZB info* [online]. 2008 [cit. 2012-04-29]. ISSN 1801-4399. Dostupné z: <http://www.tzb-info.cz/5011-autonomni-hlasice-koure>
- [19] Stabilní hasicí zařízení plynové. *Fass s.r.o.* [online]. © 2001 - 2009 [cit. 2012-04-29]. Dostupné z: <http://www.fass.cz/cs/Stabilni-hasici-zarizeni-plynove-GHZ-17.htm#kd1230>
- [20] ŽÁČEK, Jaroslav. Zdroje nepřerušovaného napájení – UPS. *Elektro: odborný časopis pro elektrotechniku* [online]. 2001, č. 10 [cit. 2012-04-05]. ISSN 1210-0889. Dostupné z: http://www.odbornecasopisy.cz/index.php?id_document=23907
- [21] Referenční návrh UPS s dsPIC. In: *Pandatron: Elektrotechnický magazín* [online]. c) 2000 - 2012 [cit. 2012-05-01]. ISSN 1803-6007. Dostupné z: http://pandatron.cz/?3000&referencni_navrh_ups_s_dspic
- [22] TURTURRO, Gianluca. *GTblog* [online]. © 2009 - 2012 [cit. 2012-04-05]. Dostupné z: <http://blog.gtweb.cz/>
- [23] *Laka cz: Klimatizace a repelná čerpadla* [online]. © 2010 [cit. 2012-05-01]. Dostupné z: <http://www.laka.cz/>
- [24] *Klimatizace T&SC* [online]. © 2011 – 2012 [cit. 2012-03-24]. Dostupné z: <http://www.klimatizace-tsc.cz>
- [25] Princip Klimatizace. *TopR klima* [online]. © 2012 [cit. 2012-03-27]. Dostupné z: <http://www.topr-klima.cz/princip-klimatizace/>

-
- [26] *Zálohování* [online]. 2010 [cit. 2012-05-01]. Dostupné z: <http://www.zalohovani.net/>
- [27] PFEIFER, René. Zálohování stokrát jinak. In: *Svět hardware* [online]. 2009 [cit. 2012-05-01]. ISSN 1213-0818. Dostupné z: http://www.svethardware.cz/art_doc-FD7558DFBCEAA617C12575BE0024AE45.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AAC	Automatic Air Conditions
ACS	Access Control System
CCTV	Close Circuit Television
CD	Compact disk
DAS	Directly Attached Storage
DVD	Digital Video Disk
EDA	Equipment Distribution area.
EM	Elektromagnetismus
EPS	Elektrická požární signalizace
eSATA	external SATA
EZS	Elektrické zabezpečovací systémy
FC	Fiber Channel
FTP	File Transfer Protocol
GSM	Global System for Mobile Communication
HDA	Horizontal Distribution area.
I&HAS	Intruder and Hold-Up Alarm System
iSCSI	internet SCSI
IT	Information Technology
LAN	Local Area Network
LED	Light Emitting Diode
MDA	Main Distribution area.
MDPO	Minimální doba průlomové odolnosti
MW	Microwave
MZS	Mechanické zábranné systémy

NAS	Network Attached Storage
PATA	Parallel Advanced Technology Attachment
NP	Nadzemní patro
OS	Operation System
PC	Personal Computer
PIR	Passive Infra-Red
PZTS	Poplachové zabezpečovací a tísňové systémy
R	Rádio
RAID	Redundant Array of Inexpensive/Independent Disks.
RFID	Radio Frequency Identification
SAN	Storage Area Network
SAS	Serial Attached SCSI
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SD	Secure Digital
SHZ	Stabilní hasicí zařízení
SMS	Short Message System
TCP/IP	Transmission Control Protocol / Internet Protocol
TV	Televize
UPS	Uninterruptible Power Systems
US	Ultrasonic
USB	Universal Serial Bus
VFD	Voltage and Frequency Dependent
VFI	Voltage and Frequency Independent
VI	Voltage Independent

VZT Vzduchotechnika

WAN Wide Area Network.

ZDA Zone Distribution Area

SEZNAM OBRÁZKŮ

Obrázek 1: Struktura datového centra [2]	15
Obrázek 2: Schéma technologie DAS.....	17
Obrázek 3: Schéma technologie SAN [4]	18
Obrázek 4: Schéma technologie NAS.....	19
Obrázek 5: Schéma fyzické bezpečnosti datového centra.....	20
Obrázek 6: Rozdělení MZS.....	23
Obrázek 7: Datový sejf	25
Obrázek 8: Média sejf.....	26
Obrázek 9: Zabezpečený rack	27
Obrázek 10: Datová komora [9]	28
Obrázek 11: Rozdělení PZTS.....	29
Obrázek 12: Princip magnetického kontaktu [8].....	34
Obrázek 13: Vlnová délka.....	35
Obrázek 14: Vlnová délka viditelného spektra.....	36
Obrázek 15: a) Fresnelova čočka b) klasická čočka	36
Obrázek 16: Vyzářovací charakteristika - malý výkon (A), vyšší výkon (B) [8]	37
Obrázek 17: Odkrytovaná ústředna [12]	39
Obrázek 18: Schéma dvojité vyvažované smyčky	40
Obrázek 19: Ukázka systému kontroly vstupu [13]	42
Obrázek 20: Terminál docházkového systému [14]	43
Obrázek 21: Čip v podobě přívěsku ke klíčům	45
Obrázek 22: Čtečka čipové karty s klávesnicí [14]	45
Obrázek 23: Personalizační čtečka	46
Obrázek 24: Ústředna EPS [17].....	49
Obrázek 25: Tlačítkový hlásič	50
Obrázek 26: Princip ionizační komory.....	51
Obrázek 27: Spínání tmou.....	52
Obrázek 28: Spínání světlem [18]	52
Obrázek 29: Schéma SHZ.....	54
Obrázek 30: Jednoduchá jednotka UPS.....	55
Obrázek 31: Schéma off-line UPS.....	56

Obrázek 32: Schéma line-interactive UPS	57
Obrázek 33: Schéma on-line UPS [21].....	58
Obrázek 34: Paralelní zapojení jednotek UPS.....	59
Obrázek 35: Split systém	61
Obrázek 36: Oblasti pro freecooling.....	62
Obrázek 37: Poměr odvlhčení	63
Obrázek 38: Poměr kolísání teplot	64
Obrázek 39: Poměr průtoku vzduchu.....	64
Obrázek 40: Teplá – studená ulička.....	66
Obrázek 41: Zdvojený strop.....	66
Obrázek 42: Oddělení klimatizačních jednotek	67
Obrázek 43: Ukázka kódu dávkového souboru	76
Obrázek 44: Výpis příkazové řádky po spuštění dávkového souboru.....	77
Obrázek 45: Základní zobrazení plánovače úloh – MS Windows 7	78
Obrázek 46: Základní nastavení NetBak Replicatoru	79
Obrázek 47: Připojení k NAS serveru	80
Obrázek 48: Základní rozhraní NetBak Replicatoru	80
Obrázek 49: Označení adresářů k zálohování	81
Obrázek 50: Nastavení rozvrhu zálohování	82
Obrázek 51: Uložení nastavení.....	82
Obrázek 52: Obecné nastavení zálohování.....	84
Obrázek 53: Nastavení zálohovaných adresářů a souborů.....	85
Obrázek 54: Nastavení komprese a šifrování záloh.....	86
Obrázek 55: Přehled vlastností zvolené úlohy.....	87
Obrázek 56: Poloha objektu.....	89
Obrázek 57: Letecký snímek okolí objektu.....	89
Obrázek 58: Půdorys 1NP	90
Obrázek 59: Půdorys 2NP	91
Obrázek 60: Rozmístění prvků 1NP	99
Obrázek 61: Rozmístění prvků 2NP	100

SEZNAM TABULEK

Tabulka 1: Míra rizika.....	30
Tabulka 2: Stupeň zabezpečení	31
Tabulka 3: Třída prostředí	31
Tabulka 4: Hustota tepelného zatížení.....	66
Tabulka 5: Porovnání zálohovacích metod	83
Tabulka 6: První poschodí	92
Tabulka 7: Druhé poschodí.....	93
Tabulka 8: Stanovení stupně zabezpečení.....	94
Tabulka 9: Přehled zón	98

SEZNAM PŘÍLOH

Příloha P I: Rozpočet

Příloha P II: Návrh dalších opatření

Příloha P III: Použité schematické značky

Příloha P IV: Certifikáty prvků systému

Příloha P V: Obsah disku CD

PŘÍLOHA P I: ROZPOČET

Typ prvku	Označení	Počet kusů	Cena za ks	Cena celkem
PIR detektor	<i>DM50</i>	22	660 Kč	14 520 Kč
Magnetický kontakt	<i>ZC1</i>	25	699 Kč	17 475 Kč
Vnitřní siréna	<i>SA913F</i>	2	219 Kč	438 Kč
Venkovní siréna + akumulátor	<i>PS-128 SIGNAL + AKKU 7Ah</i>	1	1 499 Kč	1 499 Kč
Detektor tříštění skla	<i>DG457 GLASSTREK</i>	2	699 Kč	1 398 Kč
Detektor CO ₂	<i>GD983-CO</i>	1	899 Kč	899 Kč
Detektor zemního plynu	<i>GD986-NG</i>	1	899 Kč	899 Kč
Expandér pro 4 smyčky	<i>ZCX4</i>	1	829 Kč	829 Kč
komunikátor GPRS/IP	<i>PCS300/IP</i>	1	3 199 Kč	3 199 Kč
Akumulátor	<i>AKKU SMART 12V/2,3Ah</i>	1	285 Kč	285 Kč
Ústředna + kl8vesnice	<i>EVO192 + BOX S-40 + K641</i>	1	5 699 Kč	5 699 Kč
Elektromechanický zámek	<i>DZ-12VDC</i>	3	699 Kč	2 097 Kč
Videotelefon	<i>Sada DU-06</i>	1	6 499 Kč	6 499 Kč
Docházkový terminál	<i>TAC-02-ID</i>	1	6 590 Kč	6 590 Kč
Přístupový terminál	<i>SCR100</i>	1	3 999 Kč	3 999 Kč
Čtečka karet + otisků prstů	<i>SF101</i>	1	5 799 Kč	5 799 Kč
Modul pro ACS	<i>ACM12</i>	1	2 599 Kč	2 599 Kč
SW Docházka 50 + licence	<i>SW VAR-NET 50</i>	1	12 490 Kč	12 490 Kč
IP kamera	<i>FB-100Ae</i>	4	8 999 Kč	35 996 Kč
NAS server	<i>CELVIN Q800 + 8TB</i>	1	32 196 Kč	32 196 Kč
Součet				155 405 Kč

PŘÍLOHA P II: NÁVRH DALŠÍCH OPATŘENÍ

Mechanické zábranné systémy

1) Bezpečnostní fólie

- Doporučená firma:
Trieste, a.s.
Bezručova 53
763 02 Zlín-Malenovice
mobil: 775 950 950
tel./fax: 577 107 185-186
e-mail: *films@trieste.cz*
web: *www.trieste.cz*

2) Zabezpečené racky

- Doporučená firma:
COMPLETE CZ, spol. s r.o.
Tuřanka 115
627 00 Brno
tel.: 777 929 987
fax: 273 132 540
e-mail: *brno@completecz.cz*
web: *www.completecz.cz*

3) Bezpečnostní dveře

- Doporučená firma:
MRB Sazovice, spol. s r.o.
Sazovice 191
763 01 Mysločovice
tel: 577 112 511
fax: 577 112 519
e-mail: *mrb@mrb.cz*
web: *www.dverebedex.cz*

Chlazení a klimatizace

Doporučená firma:

COMPLETE CZ, spol. s r.o.

Tuřanka 115

627 00 Brno

tel.: 777 929 987

fax: 273 132 540

e-mail: brno@completecz.cz

web: www.completecz.cz

Záložní napájení

Jako záložní zdroj elektrické energie se doporučuje dieselařegát umístěný vně budovy pro lepší odvod spalin a umístěný pod krytem – ochrana před vlivy počasí. Hlavní ovládání dieselařegátu bude umístěno vedle přípojkové skříně.

Doporučený dieselařegát:

Dieselařegát Broadcrown BCJD 90

- motor John Deere
- alternátor NewAge Stamford
- řídicí panel DeepSea Electronic
- jmenovité napětí: 3x230V / 400V
- počet fází 3
- výkon při nepřetržitém provozu 64 kW
- standby výkon (max 300h nepřetržitého provozu, celkem 500h / rok) 72 kW

Výkon UPS se většinou udává ve VA, což je zdánlivý výkon. Pro přepočítání na činný výkon ve W se používá účinník, který se pro počítačovou zátěž pohybuje kolem 0,7. Dále je nutné počítat s alespoň 20% rezervou. Tzn., že na rack se zatížením cca 3 kW je zapotřebí UPS s minimálním výkonem: $(3 \text{ kW} \times 1,2) \div 0,7 = 5,14 \text{ kVA}$

doporučené UPS:

UPS Powerware 9120

- výkon 6000VA (6 kVA)
- doba zálohování 10minut
- technologie on-line

Stabilní hasicí zařízení

Doporučená firma:

Euroalarm

U zimního stadionu 4286

760 01 Zlín

tel.: 577 217 061











777 705 712





fax.: 577 700 720


e-mail: zlin@euroalarm.cz

web: www.euroalarm.cz

PŘÍLOHA P III: POUŽITÉ SCHEMATICKE ZNAČKY

Značka	Zkratka	Popis
	MG	Magnetické čidlo otevíření
	PIR	PIR vějíř
	PIR D	PIR dlouhý dosah
	DTS	Čidlo rozbití skla (detektor tříštění skla)
	KL	Ovládací klávesnice (ovladač EZS)
	GH	Hlásič úniku plynu ("GAS")
	SI	Siréna vnitřní s blikáčem (výstražné zařízení)
	SE	Siréna vnější s blikáčem (výstražné zařízení)
	EXP	Expandér, linkový modul, koncentrátor
	US	Ústředna EZS

Značka	Zkratka	Popis
	VT	Vstupní videotelefon
	DT	Docházkový terminál
	PT	Přístupový terminál
	RD	Čtečka karet (otisků)

Značka	Zkratka	Popis
	CAM IP	IP kamera

PŘÍLOHA P IV: CERTIFIKÁTY PRVKŮ SYSTÉMU

PROHLÁŠENÍ O SHODĚ

Dovozce	VARIANT plus, spol. s r.o., U Obůrky 5, 674 01 TŘEBÍČ, CZECH REPUBLIC IČO: 46967168, DIČ CZ-46967168
Druh výrobku	Infrapasivní detektor
Typ výrobku	DM50
Výrobce	PARADOX SECURITY SYSTEMS, 780 Industrial Blvd., St-Eustache, Montreal, Quebec, CANADA
Použití výrobku	Výrobek je určen pro elektronické zabezpečovací systémy
Prohlášení	Prohlašujeme, že u uvedeného výrobku byla posouzena shoda vlastností s technickými požadavky výrobku stanovenými zákonem č. 22/1997 Sb. v platném znění a technickými předpisy. Potvrzujeme, že vlastnosti zařízení splňují požadavky dle níže uvedených nařízení vlády a že výrobek je - za podmínek obvyklých a v technické dokumentaci určených - bezpečný a jsou přijata opatření pro zabezpečení shody všech výrobků uvedeného typu s technickou dokumentací.
Nařízení vlády	Uvedený výrobek je ve shodě s nařízením vlády 616 / 2006 dle níže uvedených norem.

Uvedený výrobek splňuje podmínky těchto norem

Dle autorizované osoby	Na základě níže uvedených zkušebních protokolů odpovídá výrobek těmto normám ČSN CLC/TS 50131-2-2, ČAP P 131-2-2, ČSN EN 50131-1
Zkušební protokol	2215 6471 kód 312 ze dne 3. 6. 2008 s platností do 22. 5. 2011 Vydala akreditovaná zkušební laboratoř č. 1172, TESTALARM Praha s.r.o., zkušebna EZS, Božanovská 2098, 193 00 Praha 9 – H. Počernice
Dle výrobce	Na základě prohlášení o shodě vydaného výrobcem, odpovídá zařízení těmto normám TBR-21: 1998, EN 55022: 1998, třída B, EN 50130-4: 1998, EN 60950: 1999-2000, 3. vydání

Prohlášení o shodě bylo vydáno v TŘEBÍČI dne 22. 2. 2009



Za VARIANT plus, spol. s r. o.
Ing. Juraj Urbančík
Jednatel

TESTALARM Praha s. r. o.

zkušebna EZS
Božanovská 2098
Horní Počernice
193 00 Praha 9



Č.j.: TAP-4/2008

OSVĚDČENÍ

O KLASIFIKACI ZAŘÍZENÍ
ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE
(nad rámec akreditace zkušební laboratoře dle ČSN EN ISO/IEC 17025)

Držitel:	VARIANT plus, spol. s.r.o. U Obůrky 5, 674 01 TŘEBÍČ	
IČO	46967198	
Název zařízení:	Infrapasivní detektor	
Typové označení:	DIGIPLEX DGP2-50 (BUS)	výrobce: PARADOX SECURITY SYSTEMS
Čís. protokolu:	2215 6471 Kód : 312	ze dne: 3.6.2008

Na základě výsledků zkoušek, provedených v akreditované zkušební laboratoři č.1172 - TESTALARM Praha bylo uvedené zařízení posouzeno a

ověřeno,

že podle příslušných článků ČSN EN 50131-1 a dále uvedených norem (technických specifikací apod.)

ČSN CLC/TS 50131-2-2,
ČAP P 131-2-2

vyhovuje

stanoveným požadavkům pro jeho použití v objektech s následujícím stupněm zabezpečení.

Stupeň:	2	Riziko:	Nízké až střední
Podmínky používání:	Funkce zařízení byla ověřena pro třídu prostředí II dle ČSN EN 50131-1		
Platnost osvědčení:	od 3.6.2008	do 22.5.2011	

Osvědčení je vystaveno pro potřeby NBÚ k vystavení certifikátu dle §46 Zákona č. 412/05 Sb. a certifikačního orgánu CO TT.

Prohlášení: Proti tomuto osvědčení lze podat námitky do 15 dnů ode dne doručení u zkušební laboratoře TESTALARM PRAHA. Osvědčení může být reprodukováno jediné celé a oboustranně.

Datum: 3.6.2008

Razítko a podpis:



Zbýlé certifikáty je možné najít na přiloženém disku CD (viz Příloha P V: Obsah disku CD).

PŘÍLOHA P V: OBSAH DISKU CD

Diplomová práce: Návrh zabezpečení datového centra a zajištění zálohování dat pomocí úložiště dat na síti

(:\DP-zabezpeceni_DC.doc)

(:\DP-zabezpeceni_DC.pdf)

Výkres návrhu zabezpečení (Autodesk Autocad)

(:\prilohy\vykres.dwg)

Certifikáty:

Certifikát NBÚ pro detektor tříštění skla DG457 GLASSTREK

(:\prilohy\NBU\DG457_GLASSTREK.pdf)

Certifikát NBÚ pro ústřednu DIGIplex EVO 192

(:\prilohy\NBU\DIGIplex_EVO192.pdf)

Certifikát NBÚ pro PIR detektor pohybu DM50

(:\prilohy\NBU\DM50.pdf)

Certifikát NBÚ pro magnetický kontakt ZC1

(:\prilohy\NBU\ZC1.pdf)

Certifikát shody pro detektor tříštění skla DG457 GLASSTREK

(:\prilohy\Shoda\DG457_GLASSTREK .pdf)

Certifikát shody pro ústřednu DIGIplex EVO 192

(:\prilohy\Shoda\DIGIplex_EVO192.pdf)

Certifikát shody pro PIR detektor pohybu DM50

(:\prilohy\Shoda\DM50.pdf)

Certifikát shody pro elektromechanický zámek DZ-12 VDC

(:\prilohy\Shoda\DZ_zamky.pdf)

Certifikát shody pro detektor úniku oxidu uhelnatého GDA-930-CO

(:\prilohy\Shoda\GDA-930-CO.pdf)

Certifikát shody pro IP kameru FB-100Ae

(:\prilohy\Shoda\IP_kamery_FB-xxx.pdf)

Certifikát shody pro komunikátor PCS 300

(:\prilohy\Shoda\PCS300.pdf)

Certifikát shody pro venkovní sirénu PS-128 SIGNAL

(:\prilohy\Shoda\PS-128_SIGNAL.pdf)

Certifikát shody pro vnitřní sirénu SA-913F

(:\prilohy\Shoda\SA-913F.pdf)

Certifikát shody pro přístupový terminál SCR 100

(:\prilohy\Shoda\SCR100_access.pdf)

Certifikát shody pro čtečka otisků prstů a karet SF 101

(:\prilohy\Shoda\SF101.pdf)

Certifikát shody pro docházkový terminál TAC-02

(:\prilohy\Shoda\TAC-02_access.pdf)

Certifikát shody pro vstupní videotelefon DU-06TZS

(:\prilohy\Shoda\VideoTelefon-WRT.pdf)

Certifikát shody pro magnetický kontakt ZC1

(:\prilohy\Shoda\ZC-1.pdf)

Certifikát Test alarmu pro detektor tříštění skla DG457 GLASSTREK

(:\prilohy\TestAlarm\DG457_GLASSTREK.pdf)

Certifikát Test alarmu pro ústřednu DIGIPLEX EVO 192

(:\prilohy\TestAlarm\DIGIPLEX_EVO192.pdf)

Certifikát Test alarmu pro PIR detektor pohybu DM50

(:\prilohy\TestAlarm\DM50.pdf)

Certifikát Test alarmu pro vnitřní sirénu PS-128 SIGNAL

(:\prilohy\TestAlarm\PS-128_SIGNAL.pdf)

Certifikát Test alarmu pro magnetický kontakt ZC1

(:\prilohy\TestAlarm\ZC1.pdf)