VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNIHO INŽENÝRSTVÍ
ÚSTAV AUTOMATIZACE A INFORMATIKY

FACULTY OF MECHANICAL
INSTITUTE OF AUTOMATION AND COMPUTER SCIENCE

PŘÍSTUPOVÉ ZABEZPEČOVACÍ SYSTÉMY V AUTOMATIZACI BUDOV

TITLE OF DIPLOMA THESIS

DIPLOMOVÁ PRÁCE
MASTER´S THESIS

AUTOR PRÁCE Bc. Pavel Troják
AUTHOR

VEDOUCÍ PRÁCE Ing. Daniel Zuth
SUPERVISOR

BRNO 2009

ZADÁNÍ ZÁVĚREČNÉ PRÁCE

(na místo tohoto listu vložte originál a nebo kopii zadání Vaši práce)

ABSTRAKT

Tato práce se zabývá problematikou automatizace budov, uvádí možnosti automatizace v dnešních inteligentních budovách. Podrobněji je zde řešena problematika automatizace budov u zabezpečovacích a přístupových systémů. Práce obsahuje základní pravidla těchto systémů a postup při realizaci přístupových a zabezpečovacích systémů.

Cílem této diplomové práce je návrh přístupového a zabezpečovacího systému budov. Součástí práce je také vytvoření modelu, na kterém bude prakticky předveden přístupový a zabezpečovací systém. Tento model bude sloužit firmě ELMONT GROUP a.s. jako podklad pro řešení zakázek.

ABSTRACT

This thesis deals with automation of buildings, provides the possibility of automation in today's intelligent buildings. The issue of building automation for security and access systems is solved in details. This thesis contains the basic rules of the systems and procedure in the implementation of access and security systems.

The target of this thesis is the proposal of the access and security system for buildings. Part of the thesis is also creating a model, on which will be presented the access and security system. This model will be used by the company ELMONT GROUP as a basis for dealing with contracts.

KLÍČOVÁ SLOVA

Integrovaná nevýrobní automatizace, automatizace budov, přístupové systémy, zabezpečovací systémy, systém CONCEPT.

KEYWORDS

Integrated non-productive automation, building automation, access systems, security systems, system CONCEPT

PODĚKOVÁNÍ

Děkuji Ing. Danielu Zuthovi za metodické vedení a podmětné připomínky při vypracování mé závěrečné diplomové práce. Zároveň děkuji vedení fakulty FSI VUT, že mi umožnila tuto práci vypracovat. Také bych chtěl poděkovat firmě ELMONT GROUP a.s., zejména panu Zbyňkovi Navrátilovi za podporu, financování práce a poskytnuté rady při sestavování modelu, který je součástí této diplomové práce.

OBSAH

SEZNAM OBRÁZKŮ

1 Úvod

Tato práce se zabývá přístupovými a zabezpečovacími systémy budov. Součástí práce je vytvoření modelu, na kterém budou demonstrovány některé možnosti automatizace budov. Automatizace budov patří do kategorie nevýrobních automatizačních procesů.

Automatizace budov je rychle se rozvíjející obor elektrotechniky, který vzhledem k poměrně vysokým pořizovacím nákladům nacházel ze začátku uplatnění především v hotelových komplexech a v administrativních budovách majetných firem. V dnešní době jsou ceny těchto systémů přijatelné pro širší skupinu lidí, a tak se automatizace budov objevuje v komerčních prostorech, běžných kancelářských objektech, ale také rodinných domech a bytech. Zájem o tento obor stále stoupá a díky tomu se tento obor dál a dál rozvíjí velkou rychlostí. Na trhu je mnoho firem, které se zabývají vývojem a prodejem novějších a inteligentnějších technologií. Dovednosti jednotlivých systémů jsou si velmi podobné, jednotlivé firmy se předhánějí v tom, která firma nabídne o něco víc nebo který systém je o trochu lepší. Důležitým faktorem pro získání zákazníka je i cena, a ta stále klesá. Díky těmto skutečnostem se tento obor stává zajímavější pro širší skupinu veřejnosti. Dnes je běžné při výstavbě nových budov, ať už administrativních a obchodních center, budov pro veřejnost nebo objektů pro bydlení, že stavitelé a projektanti berou automatizaci systémů budov jako standardní součást instalace, na kterou nesmí zapomenout. Výhody použití si dnes lidé uvědomují, a to i v souvislosti se stálé se zvyšujícími cenami za energie. Automatizace budov nám přináší nižší náklady na energii, větší bezpečnost osob, ochranu majetku před požárem či poškozením nebo odcizením, umožňuje řízení energetických systémů, monitorovaní aktuálních stavů a procesů v budově, a to jak místně, tak vzdáleně a také zvyšuje komfort ovládání různých technologií.

Volba systému automatizace budovy hraje důležitou roli také z hlediska otevřenosti či uzavřenosti zvoleného systému. Uzavřený systém většinou umí komunikovat jen s prvky daného systému. To může být někdy nevýhoda pro budoucí rozšíření tohoto systému či snahu propojení s jiným systémem. Opakem uzavřeného systému je systém otevřený. Tento systém je již více benevolentní k rozšiřování, modernizaci nebo propojování s jinými systémy. Můžeme propojit dokonce několik systémů dohromady. To je velmi výhodné jak po ekonomické stránce, tak po technické stránce.

Některé firmy zabývající se touto oblastí zaručují spolupráci dnes používaných prvků (hardware a software) s obdobnými prvky vyráběnými v budoucnu. Pro uživatele těchto systémů to přináší částečně ujištění, že systémy, do kterých dnes investují, mohou i nadále s odstupem času rozšiřovat, obnovovat nebo upravovat. To muže být důležité třeba při změně ovládané technologie, charakteru využití prostor nebo jiných menších změnách požadavků. Ušetříme tím náklady na změnu celého systému. Mezi takové systémy patří i systém Concept od firmy Inner Range, který byl vybrán pro vytvoření demonstračního modelu přístupového a zabezpečovacího systému.

1.1 Všeobecné rozšíření automatizace

Automatizace je dnes jedním z nejdynamičtějších technických oborů. Je začleněna jako mezioborová disciplína, a toto zařazení je pro tento obor stále více charakteristické. Začleňuje se stále více do různých oborů. Využívá nejmodernější mikroelektronické součástky a pracuje s nejnovějšími poznatky z různých oborů, a to především z elektrotechniky, počítačové techniky, informatiky a komunikační techniky. Dále také využívá poznatky z techniky pohonů, měřící techniky a zabezpečovací techniky.

Automatizace už nepatří do kategorie drahého či luxusního komfortu. Dnes je automatizace běžnou součástí výrobních linek, technologických procesu, běžných strojů a mechanismů a také nevýrobních zařízení. Využívá se v mnoha oborech a je poněkud těžké najít obor, kde se sní člověk nesetká.

Ve výrobním sektoru bude i nadále představovat prostředek pro zvyšování kvality, kvantity a tím i konkurenceschopnosti. Proto dnes řada firem zavádí nebo již zavedla automatizaci ve svých výrobních halách.

Fenoménem posledních let je zavádění automatizace do nevýrobních procesů. Sem patří třeba obor energetiky (větrné elektrárny, malé vodní elektrárny, využití sluneční energie), techniky budov (elektroinstalace, řízení osvětlení, vytápění, chladící technika, klimatizace, vzduchotechnika, zabezpečení budov, přístup do budov, ovládání výtahů, zavlažovací systémy), logistické systémy (skladové hospodářství, manipulační a dopravné systémy, parkovací a garážové systémy), technická diagnostika, automatizované měřící a monitorovací systémy dálkového ovládání a také třeba obchod (nápojové a prodejní automaty) a další obory.

S automatizační technikou se stále více setkáváme také v domácnostech při používání moderních spotřebičů (myčky, pračky). K významným směrům automatizace patří také automatizace v automobilech. S dalším vývojem informačních technologií se budeme stále více setkávat s různými druhy automatizační techniky či automatizace.

1.2 Pohled do historie

Když se podíváme do historie, kdy se začali objevovat první náznaky automatizace, tak můžeme sledovat, že tehdejší vývoj nebyl tak rychlý, jak je tomu dnes ve 21. století. Dnešní vývoj jde obrovskou rychlostí kupředu a rozmach techniky nemá hranice. Trvalo to mnoho staletí, než se technika dostala od prvních kroku zjednodušování práce a technických pomůcek k dnešní z našeho pohledu velmi moderní technice a poměrně rozsáhlé automatizaci. Nyní se podívejme do dob začátků.

Již od starověku se lidé pokoušeli svoji vlastní tvůrčí činností o zjednodušení své práce. Vzájemně si obdivovali a uznávali svoje vylepšené nástroje či díla, které jim usnadňovali jejich práci. Tyto uměle vytvořená díla, která vznikala díky lidskému myšlení, měla také nějaké automatické vlastnosti. Lidé tyto výtvory někdy považovali za zázraky a kouzla. Ulehčení lidské práce bylo často hlavní důvod, proč se o tyto věci pokoušeli. Ostatně je to dodnes velký hnací motor, který žene techniku a

automatizaci rychle kupředu.

1.2.1 Starověké technické zázraky

Ve starém Egyptě v dobách faraónů asi 200 let př. n. l. žasli lidé ve slavném městě Alexandrii nad tajemným úkazem. Otvírala se tam sama veliká, těžká, bronzová vrata chrámu. Tento zázrak nebyl ničím jiným, než jen důmyslné využití páry. Toto dílo zkonstruoval alexandrijský učenec Hérón. Hérón tak poprvé využil princip teplovzdušného motoru. Svá zařízení popsal v knize „Pneumatika“, která se zachovala až do dnešní doby.

Právě proto, že vše automatické bylo obestřeno rouškou tajemství a kouzel, lidé si neuvědomovali skutečnost, že kolem sebe vidí různé běžně používané mechanismy, které přitom také vykazovali automatické chování. Tak např. již od starodávna používali mlynáři ve svých vodních a větrných mlýnech jednoduché zařízení, které regulovalo přísun zrní mezi mlýnské kameny v závislosti na jejich otáčkách. Jestliže bylo množství zrní dodávané na mlýnské kameny příliš velké, otáčky klesaly. To bylo zajištěno hranolem, který byl umístěn na podávajícím zařízení a spojen s mlýnskými kameny. Ten ubral množství dodávaného zrní na mlýnské kameny, a tak otáčky zase stoupaly.

Bohužel právě všednost a praktičnost těchto zařízení je zbavovala příslovečného mýtu automatické výjimečnosti. Je trochu zvláštní, že ačkoliv můžeme již na příkladu ze starověké Alexandrie vidět, že lidem byla známa síla páry a teplého vzduchu, přesto až v novověku člověk využil páru tak, aby mu opravdu sloužila k ulehčení práce[13].

2 Integrovaná nevýrobní automatizace

Předmětem tohoto druhu automatizace je zavádění automatizačních procesů ve veřejných službách, veřejných obchodních sítích, zdravotnictví, peněžních ústavech, spojovacích službách, informačních službách, procesy spojené s provozem bytových a nebytových prostor a další procesy spojené například s obranou a bezpečností státu, se vzděláváním a také se šířením zpráv jak telekomunikační technikou, tak mediálními prostředky.

V současné době je tento obor stále žádanější. Automatizace je dnes na vysoké technické úrovni a při řešení konkrétních automatizačních projektů musíme k problému přistupovat komplexně. To znamená, že velmi často dochází k propojování výrobní a nevýrobní integrované automatizace. Integrovaná nevýrobní automatizace představuje jakousi paralelní větev k integrované výrobní automatizaci.

Integrovaná nevýrobní automatizace představuje tu oblast automatizace, která se zabývá automatizací nevýrobních procesů a automatizací funkcí nevýrobních soustav.

Objektivní potřeba integrované nevýrobní automatizace vyplývá ze dvou důvodů. Jednak z potřeby rovnoměrného vývoje všech oblastí automatizace. Není dost dobře možné, aby se určitá oblast automatizace vyvíjela velmi progresivně a druhá významně zaostávala. Např. inteligentní robotické systémy nemohou mít jen inteligentní řídicí systémy a současně zastaralé automatické pohony. Nebo programovatelné automaty by nemohly dobře využívat třicetidvoubitové velmi rychlé A/D převodníky a požívat málo citlivá měřící čidla a pomalé procesorové jednotky s malou operační pamětí. Složité automatizované CNC obráběcí stroje se neobejdou bez vyspělé automatické diagnostiky a automatického měření. Z toho vyplývá, že vývoj výrobní automatizace musí být doprovázen vývojem nevýrobní automatizace.

Další důvod zájmu o tento obor spočívá v její společenské objednávce. V ČR poptávka po automatických zabezpečovacích systémech představuje nejdynamičtěji rostoucí segment na trhu automatizace u nás v průběhu posledních let. Počet prodaných automobilů u nás, které jsou vybaveny náročnou a rozsáhlou automatizační technikou, bude klást v nejbližších letech velké nároky na potřebné servisní služby v oblasti diagnostiky a údržby použitých mikroelektronických automatizačních prvků. Proto současná nevýrobní automatizace má i pro naši tržní ekonomiku velký význam a odborníci v oblasti automatizace se s ní musí důkladně seznámit[3]. Dále se budeme podrobněji věnovat jedné oblasti z tohoto oboru, a to automatizaci budov.

2.1 Automatizace budov

Automatizaci budov se také jinak říká inteligentní budova. Začátky koncepce inteligentních budov sahají do 80. let minulého století. Nové tendence, zejména v komunikačních technologiích, posouvají celý obor vzájemně propojených technologií budov o zřetelný krok dopředu. Základ spočívá v propojování více technologií, jejich společném vyhodnocování a vzájemném ovládaní podle nastavených pravidel. Pojem

inteligentní budova není v současnosti vztažen k budově jako celku, ale dnes již máme na mysli bloky budov, průmyslové komplexy a často i spojení několika komplexů, ležících ve vzdálenostech mnoha kilometrů, v jiných státech či na jiných kontinentech. Základními technologiemi, tvořícími zázemí pro fungování každé budovy, jsou:

- silnoproudé systémy,
- měření a regulace (kompletní řízení vyhřívání – chlazení, optimalizace zdrojů),
- bezpečnostní systémy (elektronické zabezpečení, elektronická požární signalizace, uzavřené televizní okruhy, regulace přístupu, docházkový systém),
- telekomunikační systémy,
- automatizace pracovišť, transport.

Cílem integrace těchto technologií v inteligentních budovách je:

- maximalizovat automatizaci a snížit zásah lidského faktoru, maximálně zjednodušit obsluhu a servis,
- šetřit energii, optimalizovat procesy v budově, a tím minimalizovat náklady na provoz budovy,
- zvýšit bezpečnost,
- zvýšit užitnou hodnotu budovy, mít dokonalý přehled o stavu všech procesů budovy.

Provázání jednotlivých technologií je možné na dvou úrovních. Jejich použití vyplývá zejména z rozsahu řízení budovy a samozřejmě požadované technologie jednotlivých systémů. Úplnou samozřejmostí je také kombinace obou principů na různých úrovních (uživatele v budově A nezajímá stav klimatizace v budově B, ale platnost jeho přístupové karty již ano).

První variantou je vytvoření vazeb na úrovni komunikačního protokolu, který umožňuje použití tzv. distribuované inteligence – což znamená řízení menších celků budovy jednotlivými regulátory, které jsou vzájemně propojeny sběrnicí. Na tuto sběrnici jsou připojovány prvky jednotlivých systémů bez jakýchkoli omezení. Na jediné sběrnici jsou vedle sebe připojeny např. regulátory vytápění, čtečky přístupových karet, řízení osvětlení atd. Každý systém pracuje nezávisle na celku, ale zároveň může sdílet veškeré informace. Při podrobnějším popisu vyplyne, že lze ušetřit mnoho nákladů investičních i provozních. Druhá úroveň vazeb je na úrovni dispečerského pracoviště, které umožňuje propojení širších vazeb – např. požárního systému s přístupem a ovládáním dveří. Dispečerské pracoviště je tvořeno počítačem s řídicím softwarem, který vyhodnocuje stavy jednotlivých systémů a na jejich základě podle definovaných procesů generuje příkazy pro akci ve všech systémech. Jako komunikační médium je nejčastěji použit systém na bázi protokolu TCP/IP.
Výhody a nevýhody jednotlivých variant je nutné posoudit vzhledem k rozsahu, použitým technologiím a spolehlivosti. Systém distribuované inteligence je

spolehlivý, odolný vůči poruchám, způsobených ztrátou komunikace jednotlivých částí. Oproti tomu model propojení jednotlivých bloků na protokolu TCP/IP umožňuje integraci obrovských celků, kde se nemusíme omezovat lokalizací jednotlivých budov. Jako transportní médium může posloužit např. internet. Spolehlivost takto řešených systémů je pak ovšem závislá nejen na dostupnosti modulů, ale i na chodu mozku systému, nejčastěji PC s řídicí aplikací. Pro zvýšení spolehlivosti je proto nutné vytvořit rezervní strukturu, která přebere řízení pří výpadku systému nebo komunikační trasy.

2.2 Integrace bezpečnostních technologií

Mezi prvními systémy, které začaly tvořit uzavřený celek ještě před cíleným zaváděním systémů inteligentních budov, byly systémy zabezpečení, tj. zabezpečovací, požární a kamerové systémy doplněné řízením přístupu. Jedná se o kompaktní systémy, kde se automatizace nabízí již na základě logiky fungování jednotlivých bloků. Základním kritériem řízení funkce je přítomnost osob v budově. Pokud chceme ovládání plně automatizovat, tj. nevyžadovat od uživatele žádnou další činnost (jako je zadávání PIN apod.), je nutné rozlišit stav, kdy poslední uživatel opustí danou část budovy. Lze jej vyhodnotit dvěma základními způsoby:

- evidovat přítomnost uživatelů pomocí přístupového systému,
- detekovat ukončení pohybu osob (pomocí pohybových detektorů, kamer apod.).

Obě řešení mají své nevýhody. Budeme-li vyhodnocovat počet uživatelů logikou přístupového systému, je nutné přesné řízení průchodu osob, např. pomocí turniketů. Budeme-li vyhodnocovat pohyb v budově, lze narazit na nespočet situací, kdy tento princip selže (nedokonalost detektorů, místo bez vykrytí detektorem apod.). Dalším faktorem, jehož priorita je na místě nejvyšším, je bezpečnost. Zde máme na mysli právě opačný okamžik, kdy první uživatel vchází do budovy a systém přechází z nočního do denního režimu. Pouhá autentizace uživatele u vstupu identifikačním médiem je režim více než nebezpečný vzhledem k možnosti zcizení čipu a neoprávněného užití. Optimální cestou je dvoucestné ověření, kde druhou informací je výstup z čtečky biometrie. Již běžně používanými se staly čtečky otisků prstů, ale stále jsou zdokonalovány a cenově zpřístupňovány i jiné principy (snímače sítnice, snímače tváře). Umožňuje-li to režim budovy, je vhodné také další omezení z hlediska času a dne, ať už plné omezení, případně omezení přístupu pouze na vybrané prostory s přísným režimem.
Navrhujeme-li systém přístupu s návazností na ostatní technologie, je nutné neopomenout významný faktor, a tím je doba odezvy načtení média. Mnozí výrobci rozvíjejí existující zabezpečovací systémy dalšími nadstavbami, nejčastěji právě přístupovým systémem. Komunikační protokol pak často není (zejména v závislosti na počtu modulů) schopen poskytnout odezvu v řádu desítek až stovek milisekund, ale prodlevy se dostávají do řádu sekund, což je čas naprosto nevyhovující. Dalšími nevýhodami často bývá omezení funkčnosti s absencí rozvinutých funkcí (počítání uživatelů, dvojitý přístup apod.). Kamerový systém většinou zajišťuje pouze další stupeň ochrany, zaměřený nejen na narušitele zvenku, ale i jako ochranu proti

zneužívaní systému samotnými uživateli. Samozřejmostí musí být vzdálená správa a přístup ke kamerovému systému – a to nejen hlídací službě nebo managementu, ale i běžným uživatelům (může suplovat funkci videovrátníka) nebo zákazníkům (na vybraných kamerách může např. sledovat výrobu z kontrolních či reklamních účelů). Další možnosti se naskýtají při použití bezdrátových wifi sítí v kombinaci s PDA nebo jiným systémem přenosných počítačů[4].

2.3 Co můžeme automatizovat

- rozvod elektrické energie
- HVAC systém (vytápění, vzduchotechnika a klimatizace)
- přístupové a zabezpečovací systémy
- požární zabezpečení
- osvětlení - spínání, plynulá regulace, udržování konstantního jasu, světelné scény
- žaluzie, markýzy, rolety - ruční nebo automatické ovládání
- okna - ovládání pohonů oken (centrální otvírání/zavírání)
- audiovizuální vybavení – rozvody audia/videa
- multimediální komunikace a propojení
- simulace přítomnosti v budově, časové programy
- vizualizace stavu systému a vazba systému budovy s okolím
- dálkový odečet energií (elektroměrů, plynoměrů, vodoměrů)
- domácí hlídací systém dětí
- centrální vysavač
- ovládání vjezdové brány a vrat garáží
- ovládání vjezdových závor
- a další

2.4 Nejpoužívanější systémy

2.4.1 Osvětlení

Osvětlení můžeme řídit několika způsoby

- stav zapnuto/vypnuto (běžné spínání nebo dálkové řízení)
- regulace intenzity osvětlení světelného zdroje
- regulace intenzity osvětlení daného prostoru
- kombinace předchozích variant s autonomním řízením (senzor denního světla, senzor pohybu, časové řízení)

2.4.2 Žaluzie, markýzy, rolety

V rámci techniky systémů budov se používá stejně ovládání žaluzií nebo rolet jako ovládání osvětlení. Oba tyto druhy použití mohou být uzavřenými okruhy, ale také mohou být funkčně propojeny. Žaluzie případně osvětlení mohou být přitom

zapínány a/nebo stmívány případně ovládány:

- z místa,
- centrálně,
- dálkově ovládány pomocí infračerveného záření,
- v závislosti na čase,
- v závislosti na jasu,
- v závislosti na výskytu pohybu (osob, větru, deště, atd.).

Výhodami pro uživatele v oblasti ovládání rolet/žaluzií jsou:

- zapínáním ovládaným podle jasu, podle času a podle potřeby lze snížit náklady na energii spotřebovanou pro vytípění či umělé osvětlení;
- podmínky osvětlení ve vnitřním prostoru se dají přizpůsobit pomocí ovládání osvětlení a žaluzií v závislosti na jasech, na časovém průběhu a na potřebě tak, že se docílí pohody podle aktuálních požadavků;
- ovládáním osvětlení a žaluzií se může změnit využití prostoru bez zásahu do rozvodů.

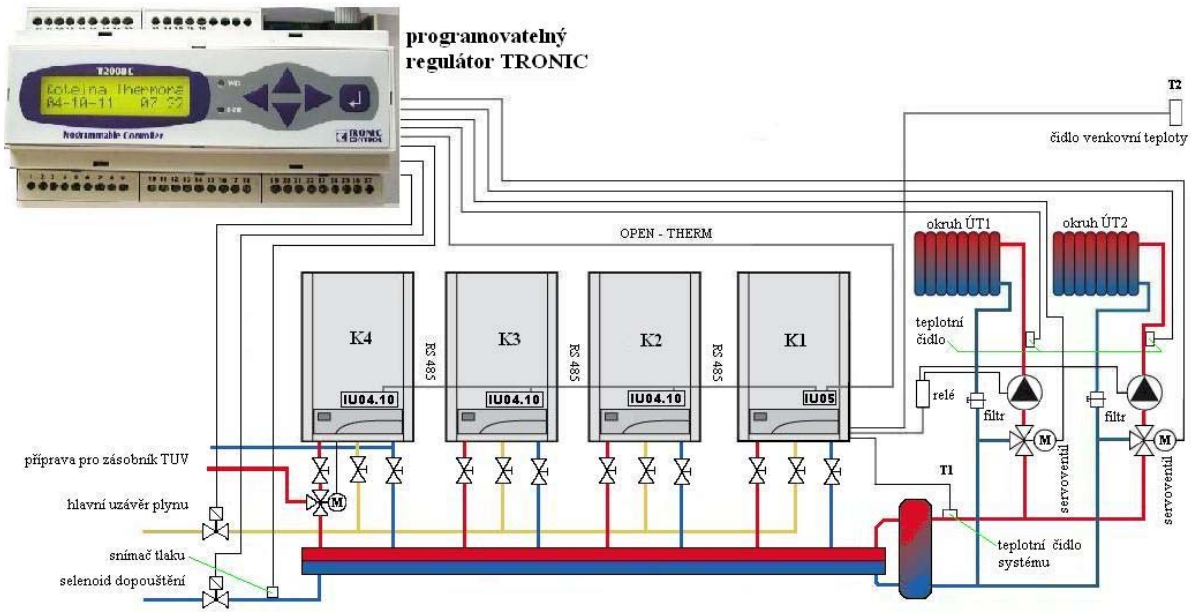
2.4.3 HVAC systémy

Jedná se o systémy vytápění, vzduchotechniky a klimatizace. Systémy řízení a monitorování HAVC v inteligentních budovách by měli vyhovovat určitým požadavkům. Požadavky jsou většinou dány již ve fázi projektování budovy. Je třeba zajistit určitá specifika na jednotlivé prostory v budově, které je třeba splnit. Prostory je třeba vytápět, větrat nebo klimatizovat dle charakteru využití. Řízení těchto systémů spolu úzce souvisí.

2.4.3.1 Příklad regulace a řízení kotelny

Na tomto příkladu regulace se jedná o kotelnu s kaskádovým zapojením kotlů. Regulace výkonu kotelny je provedena kaskádovým spouštěním kotlů. Výkon kotelny je odvozen od teploty vody na výstupu T1. Hodnota požadované výstupní teploty je nastavitelná buď jako konstantní hodnota, nebo ekvitermně závislá na venkovní teplotě T2. Spouštění kotlových čerpadel je řízeno buď přímo z regulátoru s naprogramovanou dobou doběhu, nebo společným signálem startu kotle s doběhem ovládaným časovým relé. Regulátor bude hlídat také základní zabezpečení kotlů a kotelny (vypnutí kotlů, kotelny, plynového ventilu, přehřátí prostoru, ztráta a překročení tlaku topné vody, přehřátí výstupu topné vody).

Komunikace mezi řídícím kotlem (masterem kaskády) a nadřazeným regulátorem celé kotelny probíhá přes komunikační rozhraní „OPEN - THERM“ a interface IU 05.



Obrázek 1: schéma zapojení regulace kotelny[8]

2.4.3.2 Komunikačním protokol OpenTherm®

V posledním desetiletí, kdy se digitální mikroprocesorová technika stala mnohem přístupnější, se stále častěji v řídící a regulační technice pro vytápění objevují digitální sběrnicové systémy. Všeobecně jsou tyto komunikační systémy považovány za velmi účinné a výkonné prostředky, které umožňují inteligentní řízení těch nejsložitějších otopných soustav a umožňují dosáhnout značného komfortu provozu a nízké spotřeby energií. Komplexnost a složitost těchto systémů spolu s vyšší cenou znemožňují efektivně používat tyto řídící sběrnicové systémy v běžných rodinných domcích či bytech. U otopných soustav tohoto rozsahu plně nevyhovuje oboustranná komunikace mezi prostorovým regulátorem a řídící jednotkou (hořákovou automatikou) kotle. Jednou z možností, jak tuto komunikaci zajistit, je použít jednoduchý sběrnicový systém s protokolem OpenTherm®.

Tento komunikační protokol je k dispozici u některých plynových kotlů, mezi něž patří např. kotle od firmy Thermona.
Konvenční dvoubodové prostorové regulátory pracují zcela samostatně a nezávisle na připojeném kotli. Prostorový regulátor snímá svým integrovaným čidlem teplotu v referenční místnosti vytápěného objektu a porovnává jí s hodnotou uživatelem nastavenou žádanou teplotou. Mikroprocesor prostorového regulátoru potom na základ určitého algoritmu vyhodnotí situaci a vydá řídící jednotce kotle spínací povel zapnout/vypnout. Takto je realizovaná pouze jednostranná komunikace spínacího signálu od prostorového regulátoru ke kotli.

Komunikační protokol OpenTherm® umožňuje obousměrnou dvouvodičovou komunikaci (point to point) mezi prostorovým regulátorem a řídící jednotkou kotle.

Řídící jednotka kotle zásobuje sběrnici všemi potřebnými parametry, které mohou být následně využívány prostorovým regulátorem. Prostorový regulátor je připojen na kotel dvouvodičovou sběrnicí s napájením 24 V. V tomto sběrnicovém systému pracuje prostorový regulátor jako MASTER (řídící) a interface v řídící jednotce kotle jako SLAVE (podřízený). Prostorové regulátory vybavené systémem komunikace OpenTherm® nabízejí uživateli při stejně snadném ovládání jako u dvoubodových regulátor mnohem větší přehled o systému vytápění. Může být zobrazována např. výstupní teplota kotle, aktuální výkon hořáku (procento modulace), nebo mohou být zobrazena případná poruchová hlášení. Hlavním argumentem pro použití prostorových regulátorů OpenTherm® je tzv., „druhá modulace výkonu kotle". V tomto případě kotel nemění svůj výkon pouze na základě „statického" nastavení výstupní teploty otopné vody, ale navíc je zohledněna i okamžitá prostorová teplota v referenční místnosti vytápěného objektu, které se dynamicky přizpůsobuje výkon hořáku kotle. Takto řízené nástěnné kotle dosahují v celoročním provozu úspor v řádu několika procent, snížení emisí spalin a snížení počtu startů hořáku kotle. Další úspora energie a omezení počtu startů hořáku je možná při použití ekvitermní regulace. Při této regulaci se teplota výstupní kotlové vody řídí dle aktuální venkovní teploty podle nastavené otopné křivky, což umožňuje vždy zvolit optimální výkon kotle[8].

2.4.4 Vzduchotechnika

Vhodně navržená a řízená vzduchotechnika nám zajistí tepelnou pohodu, přísun čerstvého vzduchu a samozřejmě i úspory v nákladech na vytápění a požadovanou výměnu vzduchu.

Řízení můžeme provádět např. pomocí časových programů, teploty nebo kvality vzduchu. Pro přehlednost se může provést vizualizace a řízení na počítači. Pro zvýšení bezpečnosti a stability celé technologie se řízení (regulace) vzduchotechnik provádí vždy nezávisle na vizualizačním počítači samostatným (stabilním) řídícím systémem.

2.4.5 Klimatizace

Větrací a klimatizační technika postupně zasahuje do mnoha oblastí lidské činnosti. Vývoj úpravy vzduchu, který začínal jednoduchými úpravami pro zpříjemnění života či pro zdokonalení výrobních postupů, dospěl do stavu, kdy limitovaná úroveň stavu prostředí je nedílnou součástí většiny nových produktů lidské činnosti. Každá mechanická i chemická technologie, stroj či zařízení, biotechnologie, objekty pro bydlení a shromažďování, dopravní prostředky jsou spojeny se zdroji, přenosem nebo působením látek a energií, které svojí kvalitou i kvantitou ovlivňují prostředí.
Tepelný a vlhkostní stav prostředí (resp. ovzduší), proudění vzduchu, jeho čistota a větrání (v místnostech, budovách, halách, dopravních prostředcích i uvnitř strojů a technických zařízení) patří k historicky nejsledovanějším parametrům prostředí, neboť ovlivňují bezprostředně fyzický i psychický stav člověka i funkci technologií.
Již od počátků klimatizační techniky je známo, že požadovaný stav vzduchu v místnostech může být určen ze dvou hledisek - buď požadavky osob (klimatizace pro

komfort) nebo požadavky technologickými a obdobnými, např. biologickými - rostliny, zvířata. Tyto požadavky definují parametry vzduchu (teplotu, vlhkost). Systém řízení klimatizace je obdobný jako řízení vzduchotechniky[11].

2.4.6 Audiovizuální vybavení

Řada budov bývá v současné době již vybavena několika televizory, videorekordérem, domácím kinem, audio systémem, telefony apod. Tyto systémy vyžadují svou kabeláž a instalaci. Je možné tyto systémy navzájem propojit a kombinovat jejich funkce. Rovněž je možné sdružit funkce audio/video systému s ostatními systémy. Např. je-li přijat telefonní hovor, může se automaticky ztlumit hlasitost audio/video systému.

2.4.7 Požární zabezpečení

Elektrická požární signalizace (EPS) slouží k detekci příznaků vznikajícího požáru a aktivaci návazných zařízení, které se spolupodílejí na protipožárních opatřeních. Je důležitou součástí uceleného systému protipožární ochrany objektů, ať se jedná o kancelářské budovy, výrobní provozy, hotely nebo ubytovny. Elektrická požární signalizace zajišťuje včasnou a rychlou identifikaci a lokalizaci vzniku požáru již v počínajícím stádiu hoření (zvýšená ionizace, kouř).

2.4.8 Simulace přítomnosti v budově

Systém simulace přítomnosti osob v objektu vytváří z venku dojem obydleného domu v době, kdy je dům ve skutečnosti prázdný. Každý večer se mohou např. rozsvěcovat a zhasínat světla, běžet televize nebo se pouští hudba. Ráno se třeba vytahují rolety a roztahují závěsy. Ovládat můžeme cokoliv, co je připojeno k řídícímu systému domu.

2.4.9 Vizualizace stavu systému a vazba s okolím

Při nasazení komplexního řídícího systému v budově je často požadována možnost vzdáleného sledování a ovládání objektů. Jedná se o přijímání informací o stavu budovy (hlavně o kritických a alarmních stavech – např. narušení objektu, porucha vodovodní instalace, otevření okno apod.), ale také o vzdálené ovlivňování stavu budovy (nastavení teploty místností, zapnutí pračky apod.).

Tyto požadavky je možné splnit pomocí současných komunikačních a informačních technologií:

- Síť GSM – všeobecně rozšířená síť mobilních telefonů. Její využití je velice vhodné pro vzdálené monitorování a zásahy do řízení budovy. Nejjednodušší formou je využití krátkých textových zpráv (SMS), případně systému GPRS. Budova musí být vybavena GSM modemem, který zajistí vysílání a příjem dat.
- Internet - monitorování a zásahy do řízení budovy pomocí internetových vizualizačních aplikací jsou velice komfortním a účelným způsobem ovlivňování budovy. Budova musí být vybavena internetovým rozhraním

(WEB server běžící na počítači nebo na speciálním zařízení, FTP server). Vzdálený počítač na internetu se připojí přes toto rozhraní k řídícímu systému budovy. Internetové rozhraní lze použít i pro zasílání e-mailových nebo SMS zpráv.

- Telefonní modem – pro monitorování a ovlivňování budovy lze využít i klasické pevné telefonní připojení. Toto řešení je v současnosti nahrazováno využitím GSM technologie, která nabízí lepší možnosti.
- Pagery – je možné je využít pro příjem informací o stavu budovy.

3 Ochrana objektů

Obecně můžeme ochranu definovat jako vytvoření bezpečného prostředí pro určitý subjekt. Při navrhování nějaké konkrétní ochrany musíme znát danou situaci. Musíme vědět, co chceme chránit, jak to budeme chránit a proti čemu to budeme chránit. Pro realizaci ochrany se používají prostředky, které nazýváme jednotně bezpečnostním systémem. Bezpečnostní systém můžeme rozdělit podle toho, co chráníme:

- Ochrana osobní bezpečnosti (ochrana osob)
- Informační bezpečnost (ochrana informací)
- Majetková bezpečnost (ochrana majetku)

Jako prostředek bezpečnostního systému se používají:

- Mechanické ochrany (různé mechanické zábrany)
- Elektronické ochrany (zabezpečovací systémy)
- Režimové ochrany (organizační opatření)

Při návrhu bezpečnostních systémů si musíme uvědomit, že neexistuje absolutní ochrana. Každou ochranu lze nějak překonat, záleží na znalostech a šikovnosti narušitele. Proto musíme při návrhu použít kombinaci více ochran. Nejlépe je použití všech tří výše zmíněných ochran. Mechanické ochrany pro zabránění náhodnému narušení prostor, elektronickou ochranu jako informaci o tom, že je určitý prostor narušen a také režimové ochrany pro znesnadnění vniknutí na chráněné místo.

3.1 Dělení ochran objektů dle AGA

Nejdříve si řekněme, co je to AGA (**A**sociace **G**rémium **A**larm). Asociace technických bezpečnostních služeb Grémium Alarm, o.s. je reprezentativním profesním sdružením firem a subjektů vyvíjející podnikatelskou, pracovní nebo jinou činnost v oblasti technických služeb a zařízení sloužících k ochraně osob a majetku, autorizované společenstvo Hospodářské komory ČR a členem evropské asociace EURALARM v oboru ochrany. Asociace Grémium Alarm vydala tzv. Technické informace AGA. V současné době se jedná o pět dokumentů určených především pro potřeby členské základny, zkušebních laboratoří, certifikačních orgánů, ale i uživatelů poplachových systémů. Uvedené technické informace mají normativní charakter, které odrážejí nejnovější vědecko-technické poznatky v oboru bezpečnostních systémů a služeb.

Základní dělení ochran objektů:

- Klasická ochrana – zábranné systémy

  Jedná se o ochranu dosud běžně používanou u všech objektů. Pomocí mechanických zařízení se pokoušíme chránit určitý objekt před narušitelem. K této ochraně se běžně používají mechanické zámky, západky umístěné ve stavebních prvcích. Tato ochrana se dá poměrně lehce překonat dostupnými mechanickými nástroji.

Technická ochrana

Tato ochrana navazuje na klasickou ochranu a rozšiřuje ji na vyšší úroveň. Tato ochrana sama o sobě není ochranou proti vniknutí do střežených prostor. Neumí zabránit vstupu nepovolaných osob, ale ve spojení s mechanickou ochranou umí nejen zamezit vstupu, ale i po patřičné identifikaci vpustit či zabránit osobě ve vstupu. Hlavní úkol této ochrany je podat ihned informaci o pokusu narušit nebo o narušení objektu. Lze ji charakterizovat jako detekční systém, který nám hlídá objekt a v případě narušení nám podá zprávu. Můžeme říci, že technická ochrana zvyšuje bezpečnost klasické ochrany.

Fyzická ochrana

Fyzická ochrana je završením systémové ochrany. Jedná se o ochranu prováděnou živou silou (vrátní, hlídači, bezpečnostní hlídací agentura, policie). Na její úrovni závisí výsledná účinnost všech ostatních druhů ochran. Tato ochrana je ze všech druhů ochran nejdražší. Ostatní druhy vyžadují poměrně velké počáteční investice a potom již poměrně nízkou režii. U fyzické ochrany je tomu naopak, na začátku vystačíme s poměrně nízkými náklady (výstroj), ale poté musíme počítat s vysokými náklady na režie (hlavně mzdy)[7].

Režimová ochrana

Je souborem organizačně administrativních opatření a postupů směřujících k zajištění požadovaných podmínek pro smysluplnou funkci zabezpečovacího systému a jeho sladění s provozem chráněného objektu. Režimová opatření dělíme na vnitřní a vnější.

Vnější režimové opatření se týkají především vstupních a výstupních podmínek z chráněného objektu, tj. prostorů, kudy se vozidla i osoby dostávají do objektu a kudy jej opouštějí. Jedná se především o různé vchody, vjezdy apod.

Vnitřní režimová opatření se týkají především pohybu osob a vozidel v objektu. Umožňují vstup nebo vjezd jen do některých částí prostor v závislosti na oprávněnosti dané osoby nebo vozidla. Více informací získáte

v literatuře[7].

3.2 Stupeň zabezpečení

Norma ČSN EN 50131-1 rozděluje zabezpečení na 4 stupně dle rizika:

- stupeň zabezpečení 1 pro nízké riziko (NBÚ dělení - vyhrazené)
- stupeň zabezpečení 2 pro nízké až střední riziko (NBÚ dělení - důvěrné)
- stupeň zabezpečení 3 pro střední až vysoké riziko (NBÚ dělení - tajné)
- stupeň zabezpečení 4 pro vysoké riziko (NBÚ dělení - přísně tajné)

3.3 Normy pro zabezpečovací systémy

- ČSN EN 50130 – Poplachové systémy (všeobecné požadavky)

- ČSN EN 50131 – Elektrické zabezpečovací systémy (IAS: **I**ntruder **A**larm **S**ystém) Funkce: poplachové systémy určené k detekci a signalizaci přítomnosti, vniknutí nebo pokusu o vniknutí narušitele do střežených prostor.

- ČSN EN 50132 – CCTV sledovací systémy (CCTV: **C**ircuit **C**losed **T**ele**v**ision) Funkce: poplachové systémy obsahující kamerovou sestavu, zobrazovací a další přídavná zařízení, nezbytná pro přenos signálu a obsluhu při sledování definované bezpečnostní zóny.

- ČSN EN 50133 – Systémy kontroly vstupu (ACS: **A**ccess **C**ontrol **S**ystems) Funkce: poplachové systémy, obsahující všechna konstrukční a organizační opatření včetně těch, která se týkají zařízení nutných pro kontrolu a řízení vstupů.

- ČSN EN 50134 – Systémy přivolání pomoci (SAS: **S**ocial **A**larm **S**ystems) Funkce: poplachové systémy poskytující prostředky k přivolání pomoci a které jsou určené pro použití osobami, které mohou být považovány za osoby žijící v ohrožení.

- ČSN EN 50135 – Systémy tísňové (HUAS: **H**old-**U**p **A**larm **S**ystems) Funkce: poplachové systémy, které v případě přepadení umožňují záměrné vytvoření poplachového stavu.

- ČSN EN 50136 – Poplachové přenosové systémy (ATS: **A**larm **T**ransmission **S**ystems) Funkce: poplachové systémy, které jsou především určeny k přenosu

poplachových hlašení na rozhraní poplachového systému ve střežených prostorech k rozhraní poplachového přenosového zařízení v poplachovém přijímacím centru a dále k ovládacímu a indikačnímu / zobrazovacímu zařízení v poplachovém přijímacím centru.

- ČSN EN 50137 – Systémy kombinované nebo integrované
  Funkce: poplachové systémy, které jsou kombinací jednoho nebo více jednoúčelových systémů.

4 Přístupové a zabezpečovací systémy

4.1 Přístupové systémy

Elektronický přístupový systém se používá v prostorách nebo objektech, kde je třeba zamezit vstupu neoprávněných osob, případně omezit vstup do určitých částí objektu nebo je potřebné zajistit komplexní dohled nad pohybem osob v objektu, instituci nebo areálu firmy. Přístupový systém je někdy součástí docházkového systému, kdy dochází k umožnění vstupu při evidenci příchodu. Přístupový systém dovede efektivní řízení přístupu od malých objektů s několika vstupy až po rozsáhlé systémy s tisíci uživateli. Vstupní místa jsou pro realizaci přístupového systému vybavena elektromechanickým zařízením pro jejich blokování (závory, turnikety, elektromagnetické zámky, apod.). Ovládání těchto prvků se děje pomocí výstupů, kterými jsou vybaveny všechny přístupové jednotky systému. Identifikace osob probíhá pomocí identifikačních prvků jako jsou bezkontaktní karty, magnetické karty, magnetické klíče, klávesnice, čipy, biometrické snímače (otisk prstu, geometrie ruky), pro které jsou definovány pravidla oprávnění, případně časové plány pro omezení přístupu. Tato oprávnění lze libovolně nastavovat pro jednotlivá vstupní místa. Přístupové identifikační prvky s vyhodnocovací elektronikou jsou umístěny na všechna místa, kde je třeba zabezpečit vstup pouze oprávněné osoby nebo řídit přístup osob s ohledem na jejich oprávnění.

Při průchodu tímto vstupem přiloží procházející osoba svůj identifikátor ke snímači. Na základě načtení identifikačního prvku osoby (karta, kód atd.) je proveden záznam o identifikaci a následně jsou ověřena přístupová práva jednotlivce ke vstupu do kontrolované zóny. Přístupová práva mohou být specifikována pro jednotlivce nebo skupiny i pro každou zónu individuálně včetně přesných časových vymezení. Po ověření oprávněnosti osoby dojde k uvolnění vstupu. Vstupní místa lze ovládat jednostranně i oboustranně dle potřeb provozu. Pomocí dveřních snímačů lze také monitorovat a signalizovat stav dveří.

Informace o všech událostech se přenášejí do ústředny, kde se uchovávají a zpracovávají. Výsledkem jsou přehledy o tom, kdo vstoupil, kdy, kam a na jakou dobu. Průběžně lze sledovat historii průchodů jednotlivých pracovníků a návštěvy nebo historii a frekvenci průchodů přes určité vstupy. Systémy umí evidovat a následně podávat všechny informace o nepovolených vstupech, průchodech nebo např. stavech jednotlivých dveří apod.

Příklady dalších aplikací přístupového systému:

- Ovládání výtahů s oprávněním pro jednotlivá patra
- Přístup na placená sportoviště (např. hřiště, kurty, bazény, sauny)
- Ovládání odkládacích skříněk (knihovny, fitcentra, bazény)
- Ovládání elektroinstalace např. hotelové pokoje

4.2 Zabezpečovací systémy

Elektronický zabezpečovací systém (EZS) je soubor technických prostředků, který řeší ochranu objektu proti neoprávněnému vniknutí osob na pozemek nebo do objektu. Včasnou signalizací poplachového stavu o narušení prostor na pult centrální ochrany (PCO) nebo přímo majiteli na mobil prostřednictvím SMS nebo hlasové funkce můžete eliminovat rozsah materiálních či jiných škod. Všechny tyto systémy se zpravidla skládají z několika základních prvků - zabezpečovací ústředny, ovládací klávesnice pro aktivaci a deaktivaci systému, z detektorů a z koncového zařízení, které uvědomí uživatele o narušení objektu - sirény, telefonní vyvolávače, případně komunikační systémy s pultem centralizované ochrany.

Detektory slouží k identifikaci narušení objektu. Pracují na různých principech – např. sledují infračervené záření pohybujícího se objektu vůči pozadí, detekují změny v odrazu mikrovlnného záření, využívají magnetických vlastností, snímají zvuk tříštěného skla, reagují na tlakovou vlnu, otřesy atd. Prakticky všechny detektory jsou dnes již vybaveny složitou elektronikou, která zajistí dokonalé zpracování procesu detekce a umožní prakticky eliminovat falešné poplachy.

Informace, která vznikne na výstupu detektoru je přivedena na vstup ústředny zabezpečovacího systému, která zajistí zpracování informací a následnou aktivaci výstupních obvodů. Poplachový výstup je pak přenesen na další periferní zařízení. Komunikace obsluhy s ústřednou zprostředkovává ovládací klávesnice. Ta umožní po zadání vstupního kódu aktivovat a deaktivovat zabezpečovací systém nebo jeho části.

Systém EZS může být instalován buď jako samostatná aplikace nebo jako součást dalších systémů v rámci integrace - např. systému řízení přístupu, perimetrického či kamerového systému. Objekt vybavený EZS může být zapojen do sítě pultu centralizované ochrany, kdy je objekt střežen z místa s trvalou obsluhou (ostraha objektu, policie, hlídací agentura).

Systémy EZS se může také rozšířit o systém kontroly a ochrany strážní služby, mechanické zábrany, jako jsou mříže, bezpečnostní dveře, turnikety, závory, trezory, detektory kovů a podobně.

4.2.1 Čidla elektrických zabezpečovacích systémů

Rozdělení dle funkce:

- Čidla aktivní - při zjištění změny vytváří své pracovní prostředí aktivním působením na okolí, a tak detekuje vytvořenou změnu
- Čidla pasivní - registrují pouze fyzikální změny okolí

Rozdělení podle charakteru střežení

- Prostorová – reagují na jevy související s narušením střeženého prostoru
- Směrová – reagují jen v určitém směru
- Bariérová – reagují na narušení bariéry vytvořené vyzařovací či snímací charakteristikou čidla
- Polohová – reagují na změnu polohy ochráněného prvku

Rozdělení podle dosahu

- S krátkým dosahem do 15 m
- Se středním dosahem od 15 m do 50 m
- S dlouhým dosahem nad 50 m

Rozdělení dle tvaru vyzařovací nebo snímací charakteristiky:

- Širokoúhlý rozsah
- Kruhový rozsah
- Záclonový rozsah
- Dlouhý dosah

Čidla elektronických zabezpečovacích systémů se umísťují tak, aby co nejlépe plnila svůj účel a byla montována v souladu s pokyny výrobce. Při volbě čidla musíme brát v úvahu také prostory, do kterých se čidlo instaluje z hlediska vnějších vlivů. Při nevhodné umístění čidla do prostor s vnějšími vlivy odlišnými od doporučení výrobce, nám nemusí čidlo fungovat správně. Podle umístění čidel ve střeženém prostoru můžeme dále rozdělit střežené zóny na obvodové, plášťové, prostorové, předmětové. Podle střežené zóny se volí druh použitého čidla.

Do skupiny plášťové ochrany patří tato čidla:

- Kontaktní
  - ✓ Mikrospínače (zámkové kontakty)
  - ✓ Dveřní a přechodové kontakty (dnes již málo používané)
  - ✓ Nášlapné kontakty (nášlapné koberce – fóliové, páskové)
  - ✓ Rozpěrné tyče (chrání otvory inženýrských sítí)
  - ✓ Závěsné kontakty (používají se v úzkých prostorech – např. šachty)
  - ✓ Koncové spínače
  - ✓ Magnetické kontakty (jde o nejrozšířenější čidla z této kategorie)

- Destrukční
  - ✓ Poplachové folie, tapety a skla
  - ✓ Foliové polepy (dnes se již nepoužívají)
  - ✓ Vodičové sítě a zátarasy (trezorové místnosti)
  - ✓ Světlovodné zábranné sítě (zabezpečení pláště budovy např. trezory)

- Destrukčních projevů (čidla otřesová, na ochranu skleněných ploch)
- Tlaková akustická (infrazvuková)
- Barierová (infračervené závory, záclony)

Do skupiny prostorové ochrany patří pohybová čidla:

- Mikrovlnná čidla
- VKV čidla
- Ultrazvuková čidla
- Infračervená čidla
- PIR čidla

4.2.2 PIR (Passive Infra Red) detektory

Tato čidla jsou dnes nejpoužívanějším prvkem zabezpečovacích systémů. Základem je ferroelektrický keramický senzor snímající změny tepelného pole vyvolané pohybem osob ve střeženém prostoru. Tyto změny jsou po zesílení digitálně vyhodnoceny a v případě dosažení prahové hodnoty odpovídající pohybu osoby je vyslán signál ústředně. Podobné senzory se používají např. i k automatickému ovládání světel pohybem osob. Pro aplikaci v zabezpečovacích systémech hraje velkou roli jejich směrová přijímací charakteristika, která se upravuje pomocí Fresnelových čoček z plastické hmoty.

Podle směrových charakteristik se rozlišují tři typy těchto čidel:

- Typ vějíř – nejpoužívanější směrová charakteristika, při vhodném umístění umožňuje sledování většiny prostoru v místnosti.
- Typ záclona – svislá směrová charakteristika, umožňuje sledovat průchod její rovinou, např. vstupem do střeženého prostoru.
- Typ dlouhý dosah – úzká směrová charakteristika umožňuje díky větší koncentraci tepelného pole sledování do větší vzdálenosti např. v chodbách[3].

4.2.3 Magnetické kontakty

Tato čidla monitorují pouze dva stavy (otevřeno/zavřeno) a používají se pro hlídání dveří, oken, apod. Jsou založeny na principu změn elektrického proudu procházejícího materiálem čidla poté, co se k němu přiblíží magnetické pole (polarizovaný magnet).

4.2.4 Akustická čidla

Tato čidla reagují na tříštění skla, které při porušení celistvosti, většinou skleněné plochy vyšle signál ústředně, a ta následně např. bezpečnostní agentuře. Umisťují se proti stráženému sklu (okenní tabule, výloha, apod.) a umožňují nastavit u nich různou citlivost, časovou analýzu následných zvuků a porovnávání zachycených zvuků se vzorníkem.

4.2.5 Mikrovlnná čidla

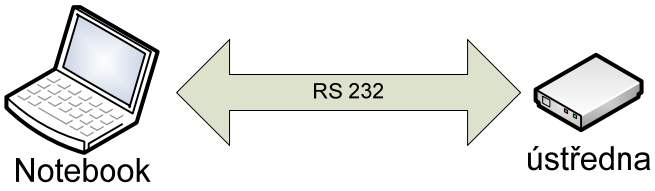
Toto čidla vysílá s nepatrným výkonem elektromagnetické záření o vysoké frekvenci a přijímají odrazy od okolního prostředí. Čidlo tyto odrazy vyhodnotí, registruje jejich změny (při pohybu) a reaguje na ně.

4.2.6 Rozhraní RS232

Rozhraní RS232 je oficiálně (podle specifikace) možné použít pro propojení dvou zařízení mezi sebou, a to jen do vzdálenosti *15* metrů při přenosové rychlosti do 20 kb/s, což vyplývá z povolené kapacity kabelu 2500 pF. V praxi jsou dosahovány výsledky mnohem lepší (115200 b/s při vzdálenosti až 50 metrů) díky použití kabelů s kapacitou pod 1000 pF.

Rozhraní RS232 je relativně málo odolné proti rušení, neboť přenos dat je realizován napěťovou úrovní na vodičích (vůči GND) na zatěžovacím odporu 3,7 kΩ při šumové imunitě 3 V. Mnoho zařízení má ale vstupní impedanci mnohem vyšší (až 30 kΩ) a šumovou imunitu nižší (1 V), takže dochází ke zvýšenému rušení, a tím ke zmenšenému možnému dosahu linky. K propojování se používá stíněný kabel a je nutno věnovat pozornost způsobu provedení signálové země a země zařízení (v plné specifikaci RS232 jsou to dva samostatné vodiče). Pro propojení dvou zařízení s rozhraním RS232 v minimální konfiguraci stačí tři vodiče (RxD, TxD, Gnd - tzv. null modem kabel), pak se ale nevyužívá řídících signálů (RTS, CTS, DSR, DTR a další). Při propojení řídících signálů počet vodičů roste podle požadavků na způsob řízení

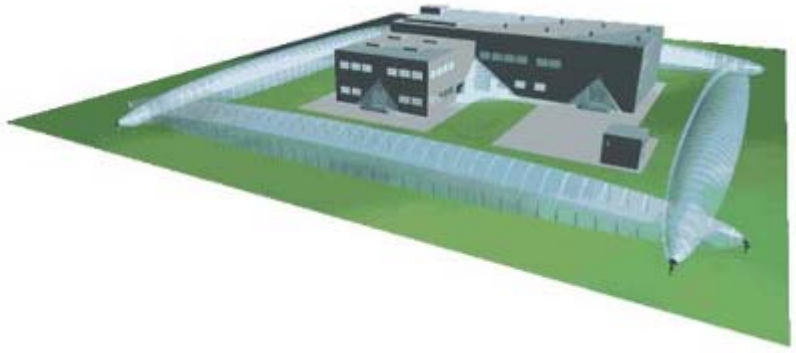
toku dat. Pro přenos dat na větší vzdálenosti se používá rozhraní *RS422* nebo *RS485*, případně proudová smyčka.



Obrázek 2: RS232

4.2.7 Perimetrické systémy

K dokonalému integrovanému systému ochrany objektů patří perimetrické systémy. Jedná se o zvláštní druh systému EZS pro střežení obvodu rozsáhlých areálů a komplexů budov, jako jsou vojenské objekty, skladové areály, letiště a velké průmyslové objekty. Perimetrický systém umožňuje zachytit narušitele ještě před vlastním vniknutím do střeženého objektu a poskytuje bezpečnostním složkám větší časový interval, který nutně potřebují k provedení zásahu.



Obrázek 3: Perimetrický systém[5]

Další velmi důležitou podmínkou při užívání perimetrických systémů je existence oplocení**,** které umožňuje definovat narušení. Bez kvalitní mechanické zábrany na hranici pozemku by mohlo docházet k nechtěnému vstupu nepovolaných osob na zabezpečený pozemek a po signalizaci poplachu by byl zásah a postih z právního hlediska velmi problematický.

Návrh a instalace perimetrických systémů je velmi specifickým problémem jak z pohledu funkce použitých technických zařízení ve velmi nepříznivých klimatických podmínkách vnějšího prostředí, tak nutnosti kombinovat a integrovat mnohem více různých prvků, než je obvyklé u ochrany vnitřní. Problémem perimetrických systémů je velké množství vlivů, na které by neměla čidla reagovat. Jsou to např. vlnění

travního porostu, pohyb listí a větví stromů a keřů, vibrace oplocení ve větru, proudění vzduchu, změny teplot, vítr, sníh a déšť, pohyby různých druhů zvěře a vlivy spojené s lidskou činností třeba i dopravní ruch v blízkosti hranice pozemku. Základním požadavkem na prvky perimetrického systému je nezávislost funkce na klimatických podmínkách[5].

5 Zabezpečovací a přístupový systém Concept

Z mnoha systémů na trhu byl použit pro bližší představení systém Concept od firmy Inner Range. Pro demonstraci byl vytvořen model, který je blíže popsán v kapitole 6. Systém Concept byl vybrán firmou ELMONT GROUP a.s., která požadovala použití tohoto systému pro sestavení modelu. Tato firma financuje všechny náklady na sestavení modelu. Zmíněná firma dlouhodobě spolupracuje s firmou Eurosat CS, spol. s r.o., která je prodejcem těchto systémů na českém trhu. Firma ELMONT GROUP a.s. se zaměřuje mimo jiné na instalaci a servis přístupových a zabezpečovacích systémů. Sestavený model bude firmě sloužit pro prezentaci systému zákazníkům a také jako výukový modul pro nové techniky.

5.1 Systém CONCEPT

Systémy Concept 4000 patří mezi oblíbené a často používané zabezpečovací a přístupové systémy, zejména ve velmi rozsáhlých instalacích. CONCEPT vyniká zejména počtem prostorů (nezávislých podsystémů), kterých může být až 250, počet uživatelů může dosahovat až 4000 (počet uživatelů, kteří jsou determinováni pouze kartou, může být více než 24 000). Velmi zajímavý je i počet zón (smyček), který může dosahovat až 4000 (nezapočítány systémové vstupy hlídající stav EZS), počet programovatelných výstupů může dosahovat maxima 3800.

CONCEPT umožňuje řešit nejenom zabezpečení objektu, ale poskytuje i funkce pro vytvoření přístupového systému. Evidenci přístupu osob lze libovolně provázat se zabezpečovacím systémem, čímž se pro uživatele značně zjednodušuje ovládání a samozřejmě také klesají náklady určené na instalaci. Velmi žádanou vlastností je i možnost spolupráce s docházkovým systémem – díky použití standardního komunikačního formátu Wiegand lze připojit libovolný docházkový terminál, který poskytuje data v tomto formátu. Uživatel tak není vázán na použití jediného typu docházkového terminálu a příslušného programového vybavení.

Možnosti nasazení však sahají dále, neboť CONCEPT nabízí další nadstandardní funkce, jako například řízení a zabezpečení výtahů. Náročné uživatele jistě zaujme možnost automatického řízení klimatizace a topení, přičemž nejsou opomenuty ani běžné funkce pro řízení jednodušších elektrospotřebičů. Mezi unikátní vlastnosti patří možnost snímání a vyhodnocování „analogových“ veličin (např. teplota, intenzita osvětlení atd.).

Jednou z nejdůležitějších vlastností každého zabezpečovacího zařízení jsou bezesporu jeho komunikační schopnosti. CONCEPT nezaostává ani v této oblasti, neboť ústředna umožňuje komunikovat s řadou zařízení, mezi ně patří v první řadě PCO, dále pak i prostředky výpočetní techniky, mobilní GSM telefony nebo lze data přenášet po LAN s protokolem TCP/IP (např. internet). Ústředna umožňuje paralelní zpracování komunikačních úloh, takže je možné současně přenášet informace na několik různých typů zařízení (současně lze přenášet zprávu na PCO, tutéž událost

tisknout na tiskárně, zobrazovat v PC, zasílat formou SMS na mobilní telefon, …).

Concept 4000 lze přes sériové rozhraní připojit k PC, na kterém běží software Insight. Pomocí tohoto programu je možné snadno konfigurovat a kontrolovat stav více ústředen, přičemž toto ovládání a nastavení může být prováděno z více koncových stanic (z tzv. klientů). Program Insight umožňuje připojení dalších programových či hardwarových modulů, které mohou podstatně rozšiřovat funkčnost systému (řízení CCTV prvků, zasílání varování e-mailem či pomocí SMS, komplexní správa uživatelských karet aj.).

Z uvedeného výčtu je patrné, že se jedná o dynamický a progresivní systém, který je připraven řešit nejen požadavky pro zabezpečení a řízení přístupu do objektu, ale i řízení technologických procesů.

5.1.1 Funkce systému

Systémy Concept představuje moderní modulární systém, umožňující vytvářet následující funkční subsystémy:

- zabezpečovací systém
- přístupový systém
- systém řízení a správy budov (řízení výtahů, řízení klimatizace)

Systém je dále schopen zcela či částečně integrovat docházkový systém (při použití docházkového terminálu ve formátu Wiegand), popř. další systémy (např. CCTV) ve spolupráci s nadřazeným PC pomocí software Insight aplikace AlViS a jiné.

5.1.2 Moduly

Systém Concept se řadí mezi modulární systémy, tzn. je rozdělen na řadu zařízení, které mají specifické funkce a které spolu vzájemně komunikují po společné LAN. Na jedné LAN jich smí být maximálně 250, přičemž až 99 modulů smí být téhož typu. K rozlišení jednotlivých zařízení na LAN se používá adresa, přičemž tato musí být jedinečná pro každý modul téhož typu. „Srdcem“ celého systému je ústředna. Toto zařízení shromažďuje veškerá konfigurační data, komunikuje se všemi ostatními moduly připojenými do LAN a na základě těchto podkladů rozhoduje o činnostech, které bude systém vykonávat.

K nastavení nebo ovládání systému se používá LCD klávesnice, vybavená podsvětleným LCD displejem a 20 klávesami. Pomocí konfiguračních voleb lze omezit, které údaje má klávesnice zobrazovat a které typy operací bude možné na vybrané klávesnici provádět. Dále je tento modul vybaven 2 vstupy a 2 výstupy, které lze použít k libovolným účelům, např. pro ovládání přístupového systému.

Univerzální expandéry s integrovaným zdrojem se využívají ke zvýšení počtu zón, auxů (výstupů) či modulovaných sirén. V základním provedení poskytuje tento

modul 16 zón, 8 výstupů (auxů) s otevřeným kolektorem a dva modulované sirénové výstupy. Po doplnění o rozšiřující modul lze počet zón zvýšit na 32, stejným způsobem lze rozšířit i výstupy (max. 32 auxů s otevřeným kolektorem). Po osazení speciálních vstupů/výstupů slouží tento modul pro ovládání přístupu výtahu do jednotlivých pater. Mini-expandéry umožňují rozšíření systému o 8 zón a 8 auxů. Mini-expandéry nejsou vybaveny vlastním zdrojem, a proto musí být napájeny z LAN nebo z externího zdroje. Vstupy (zóny) mini-expanderů umožňují používat specifické funkce – mohu například pracovat jako čítače pulsů.

Přístupové moduly slouží, jak je patrné z jejich názvu, k budování přístupového systému. Ke vstupům těchto modulů lze připojit externí snímací zařízení (čtečky karet, otisků prstů, docházkové terminály aj), které slouží k identifikaci uživatele. Na základě nastavení systému je pak rozhodnuto, zda bude či nebude danému uživateli (resp. jeho kartě) povolen přístup a zda tedy bude či nebude sepnut výstup zámku dveří (uvolnění turniketu aj.). Tento modul se vyrábí ve dvou variantách, a to buď s jedním nebo dvěma vstupy pro připojení snímačů.

Inteligentní přístupový modul umožňuje plně ovládat a monitorovat až 4 přístupové body (dveře), neboť je vybaven 4 vstupy pro připojení externích snímačů (čteček karet, otisků prstů). Modul lze rozšířit o další 4 vstupy pro připojení čteček, takže uvedené 4 přístupové body (dveře) mohou být ovládány i oboustranně. Na rozdíl od předchozích přístupových modulů je tento modul vybaven vlastní pamětí pro uchování konfiguračních dat, takže je v případě výpadku komunikace s ústřednou schopen plně pracovat a zaznamenávat vzniklé události.

Analogové moduly dovolují měřit a vyhodnocovat spojitě se měnící veličiny jako je např. teplota, intenzita osvětlení, vlhkost půdy aj. Každý analogový modul je vybaven 4 vstupy, které mohou být nezávisle nastaveny. Jelikož nemá analogový modul vlastní zdroj, je nutné jej napájet z LAN či z externího zdroje.

LAN izolátor slouží pro rozšíření či rozdělení komunikační LAN. Poskytuje galvanické oddělení mezi jednotlivými segmenty LAN, eliminuje problémy se zemními smyčkami a zlepšuje přepěťovou ochranu. LAN izolátor dále zlepšuje poměr signál/šum a zesiluje signál na velmi dlouhých kabelových trasách. Dovoluje také zapojení „do smyčky“, což zvyšuje bezpečnost LAN subsystému.

Zdroj 2,5 A je dostupný v různých provedeních. Výstupní napětí je 13,8 V, maximální odebíraný proud je až 2,5A. Na desce jsou dále obsaženy konektory pro připojení zálohovacího akumulátoru. Zdroj umožňuje detekovat ztrátu AC napájení či pokles napětí zálohovacího akumulátoru. Jednodušší typy zdrojů tyto události indikují pomocí výstupů, pokročilejší typy zdrojů tyto informace přenášejí přímo pomocí LAN.

5.1.3 Doplňující moduly systému

- Rozšiřující deska sériových portů RS232 (jeden, dva či čtyři sériové porty).

- Modulu IRC02/COM. Tento komunikační převodník je schopen překládat data z ústředny na jiný formát, používá se např. pro spojení systému Concept s objektovými zařízeními Fautor, LATIS, NAM či RADOM po sériové lince. Data z Conceptu jsou předávána pomocí rozšiřující sériové linky RS 232.

- Ethernet UART rozšuřující modul. Tento modul umožňuje pomocí TCP/IP obousměrně komunikovat mezi ústřednou a ovládacím programem INSIGHT. Touto metodou lze připojit vzdálené ústředny pomocí sítě internet.

Zde jsou uvedeny některé nejčastěji používané moduly. V systému Concept lze použít i mnoho dalších modulů pro ovládání inteligentních budov. Další informace je možné se dozvědět [9].

5.2 Popis zabezpečovacího systému CONCEPT

Základní funkcí systému Concept je zabezpečovací systém. Na rozdíl od jiných systémů byl Concept od počátku vyvíjen i jako systém přístupový, což se odráží v celkové míře možné provázanosti těchto dvou celků. Základem zabezpečovacího systému jsou vstupy (zóny), které detekují pohyb či jiné události v chráněném objektu. Zóny jsou z důvodu snazšího ovládání sdruženy do vyšších celků – prostorů (skupin, group, podsystémů). Zóny vyhlašují poplach pouze v případě, že je zapnut (aktivován, zastřežen) prostor, ve kterém jsou zóny. K zapnutí/vypnutí střežení jednotlivých prostorů slouží uživatelské kódy, které se v systému autorizují pomocí PINu či přístupové karty.

5.2.1 Základní vlastnosti zabezpečovacího systému

- Max. 2000 zón (vstupů)
- Max. 250 nezávislých prostorů (podsystémů)
- Max. 4000 uživatelů s PINem a 24576 s přístupovou kartou.
- Prostory mohou být ovládány buď jednotlivě či po skupinách.
- Programové vlastnosti umožňují ovládání prostoru uživatelem, stavem zóny, výstupem, pomocí PC, na základě časových zón, počtu uživatelů aj.

- Mohou být vytvořeny „společné“ prostory, které se automaticky aktivují po zabezpečení všech nadřazených oblastí.
- Lze použít modulované či spínané sirény, každý prostor může aktivovat jinou sirénu (resp. sirény).
- Lze nastavit různé odezvy (typy zón) na jednotlivých vstupech. V rámci typu zóny lze nastavit stavy, které má zóna zpracovávat, zda a které stavy mají být přenášeny na komunikátor, dále zda mají být aktivovány modulované výstupy sirény či spínané auxy (výstupy) a také lze nastavit, které klávesnice mají zobrazovat patřičné informace.
- Každá zóna (vstup) smí být zařazena v až 8 různých prostorech s různě definovanou odezvou.
- Systémové stavy (výpadek AC, nízké napětí baterie) jsou zpracovávány jako systémové zóny a lze tak definovat libovolnou odezvu na vznik těchto událostí.
- Uživatelé jsou sdruženi do skupin (do tzv. typů uživatelů), přičemž každému typu lze určit, které prostory a dveře smí ovládat a které funkce v systému má mít povoleny.
- Každému uživateli lze přiřadit PIN či přístupovou kartu, dále je nutné přidružit typ uživatele. Některým uživatelům lze přiřadit i jméno[9].

5.3 Popis řízení přístupu Concept

Systém Concept umožňuje vybudovat plnohodnotný přístupový systém, který může být jednoduše provázán se systémem zabezpečovacím. Základem přístupového systému jsou přístupové body, kterými lze projít až po identifikaci a následném povolení systémem (např. dveře vybavené elektromagnetickým zámkem, turnikety, aj.). Uživatelé jsou v přístupovém systému autorizováni kartou (načítána ve snímači, který je připojen k přístupovému modulu) a/nebo PINem, který lze zadat na LCD klávesnici nebo čtečkou s klávesnicí. Každým dveřím je nutné přiřadit tzv. skupinu přístupu. Tato programová volba určuje, jaké prostředky (PIN, karta, odchodová, příchodová tlačítka) slouží k otevření dveří. Dále lze nastavit časové okno, kdy bude přístup platný. Mezi další funkce patří vzájemné blokování dveří či proti-dvojí přístup (antipassback).

5.3.1 Vlastnosti přístupového systému

- Použití max. 250 dveří. Dveře mohou být primárně ovládány pomocí čtečky a přístupového modulu či pomocí LCD klávesnice.
- Počet uživatelů, vybavených pouze kartou může dosahovat až 24 576.

- Dveře mohou být dále ovládány pomocí příchodových/odchodových tlačítek, na základě stavu zóny, na základě výstupu, z ovládacího PC, dle časového nastavení.
- Po připojení detektoru, který kontroluje stav dveří, je možné vyhodnotit násilné otevření dveří či překročení povolené doby pro otevření dveří.
- Přístupový systém lze provázat se zabezpečovacím, např. automatickým vypnutím prostoru, do kterého uživatel vchází skrze konkrétní dveře nebo zamezením přístupu do dveří, které předcházejí zabezpečenému prostoru.
- Znemožnění dvojího přístup (antipassback), kdy uživatel nesmí vícekrát vstoupit do prostoru, kde se již nachází (nesmí dvakrát vstoupit ze stejné strany dveří)
- Vzájemné blokování dveří znemožňuje otevření dveří v případě, že jsou otevřeny jiné dveře či je sepnut kvalifikační výstup.

5.4 Komunikace systému Concept

Systém Concept je standardně vybaven integrovaným telefonním komunikátorem a jednou sériovou linkou (lze rozšířit až na 5 nezávislých RS 232 linek). Pomocí těchto rozhraní lze komunikovat v mnoha formátech se širokou škálou různých zařízení. Pomocí telefonního rozhraní lze předávat zprávy na PCO, komunikovat se vzdáleným modemem (pro změnu konfiguračních voleb) či používat DTMF ovládání systému. Sériová linka může předávat informace přímo v textovém formátu do připojeného PC či sériové tiskárny, pomocí speciálních komunikačních protokolů PC Direct či INSIGHT lze obousměrně komunikovat (měnit konfigurační data, monitorovat či ovládat systém). Takto lze připojit buď PC (programy INSIGHT, AlViS) nebo další externí zařízení (GSM modem, komunikační převodník IRC02/COM, RS232 - TCP/IP převodník). V jednom okamžiku smí být aktivních více komunikačních úloh. Systém umožňuje současně přenášet zprávy na PCO telefonním komunikátorem, zároveň je tisknout na sériové tiskárně a pomocí další sériové linky tyto informace předávat nadřazenému PC.

5.4.1 Komunikační vlastnosti systému

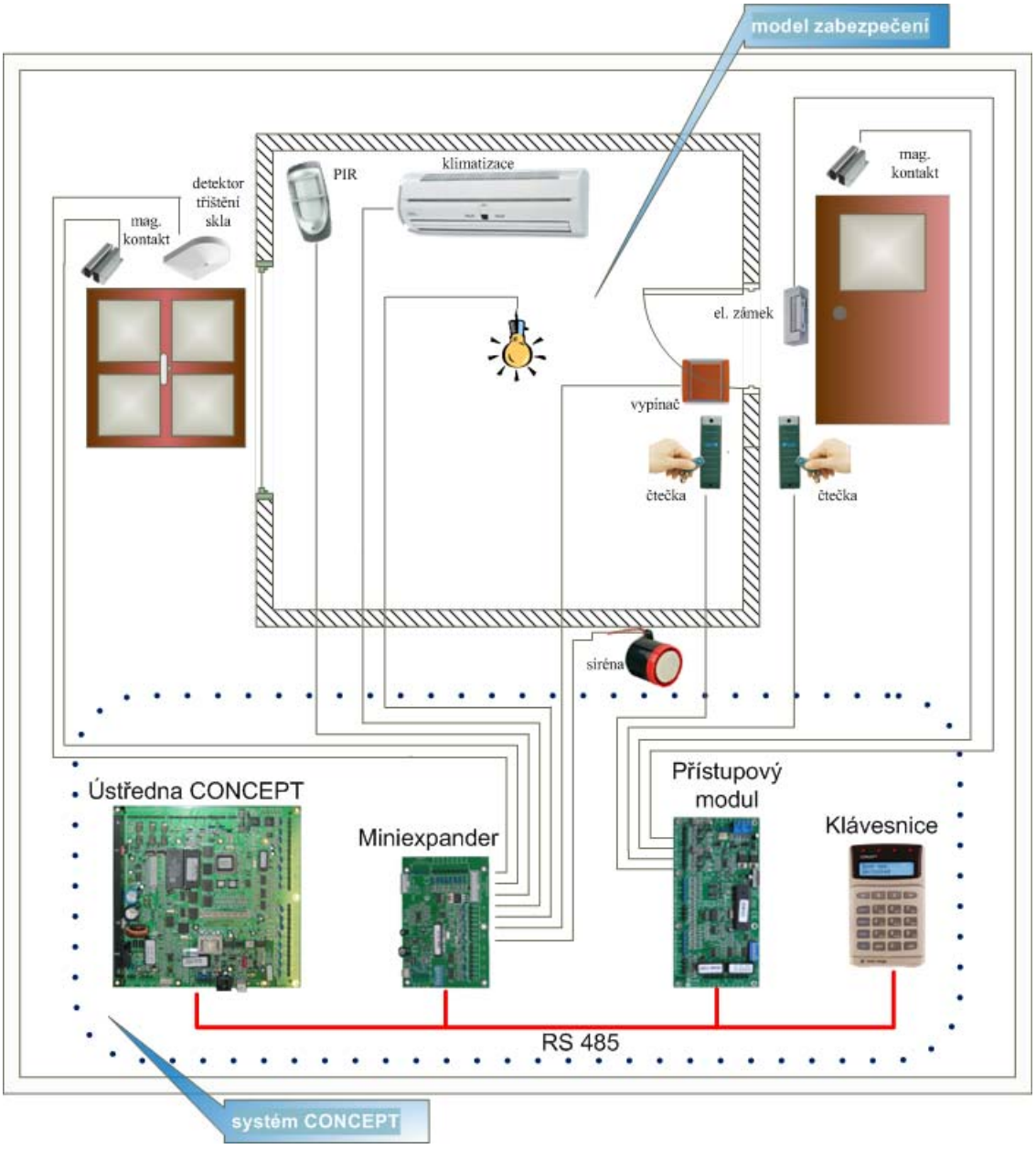
- Ústředna má integrován telefonní komunikátor a jednu sériovou linku
- Pomocí rozšiřujících portů lze počet sériových linek zvýšit na 5 a jeden TCP/IP port.
- Telefonní komunikátor může předávat zprávy na PCO
- Pomocí telefonního rozhraní je dále možné provádět vzdálený přístup přes modem a měnit konfigurační data, monitorovat stav systému či ovládat jeho jednotlivé prvky.

- Telefonní rozhraní poskytuje standardní funkce pro monitorování linky, přemostění záznamníku a zpětné volání.
- Sériové linky RS 232 mohou přenášet data do externího systému (sériová tiskárna, PC, modem, GSM modem) v textovém formátu či pomocí obousměrných protokolů WDirect, INSGIHT.
- a další.

Další informace můžete získat[9].

6 Model přístupového a zabezpečovacího systému

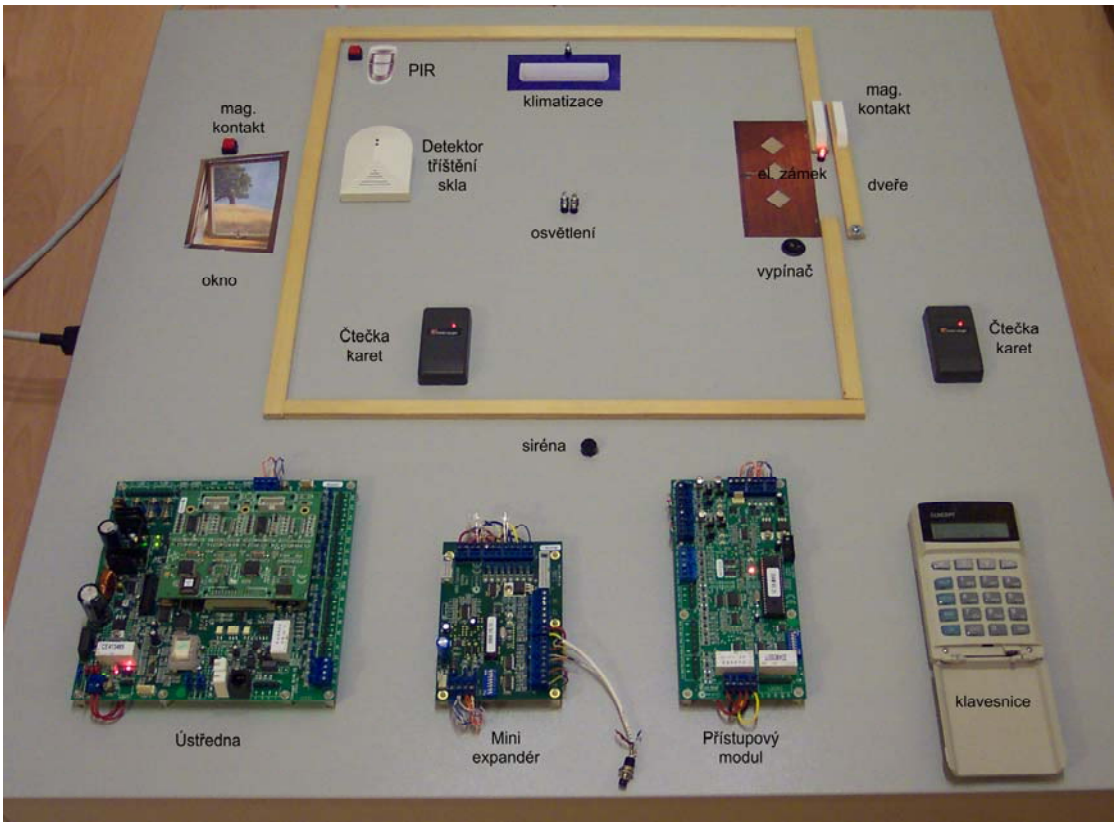
Jedním z cílů této práce je vytvoření modelu přístupového a zabezpečovacího systému. Na tomto modelu budou předvedeny prakticky jednotlivé funkce tohoto systému. Model představuje jednu místnost (např. kancelář), která je vybavena jednotlivými komponentami. Návrh konstrukce tohoto modelu je vidět na Obrázek 4: návrh modelu. Z důvodu velikosti a cenové náročnosti jsou na modelu předvedeny jen některé funkce systému. Další možnosti tohoto systému jsou v této práci uvedeny v kapitole 6.5.



Obrázek 4: návrh modelu

6.1 Konstrukce

Model je proveden na dřevěné desce o velikosti 90 x 90 cm z důvodů manipulovatelnosti a možnosti převozu. V jedné části desky jsou umístěny komponenty systému, které nejsou určeny k běžnému kontaktu s uživatelem. Jedná se především o ústřednu, hlavní prvek tohoto modelu. Dále je zde umístěn modul pro zajišťování přístupu do místnosti (přístupový modul) a modul pro zabezpečení místnosti (Mini expandér). Na spodní straně desky je umístěn napájecí zdroj – transformátor 230V/16V a vodiče pro napájení modulů a funkční zapojení jednotlivých prvků systému.



Obrázek 5: Model

Na modelu je znázorněna místnost kanceláře, ve které je z nějakého důvodu omezen a hlídán vstup osob. Tato modelová kancelář je vybavena jednotlivými komponentami sloužícími pro přístup a zabezpečení. U dveří jsou z obou stran umístěny čtečky karet sloužící pro evidenci jednotlivých osob vstupujících do místnosti a zároveň nám systém kontroluje odchod těchto osob z místnosti. Dále nám umožňuje kontrolu antipassback, což je zamezení dvojího přístupu stejné osoby. Jednoduše řečeno, ten kdo do místnosti vstoupí, musí nejdříve odejít, aby mohl opět vstoupit. U vstupních dveří je symbolicky znázorněn elektrický zámek jako signální dioda. Tato dioda nám signalizuje otevření či zavření elektrického zámku. Svítí-li dioda červeně, je zámek zajištěn a naopak, při zeleném svitu je signalizováno

otevření zámku dveří. Na dveřích je pro demonstraci namontován magnetický kontakt, který kontroluje otevření dveří.

V místnosti za dveřmi je umístěn vypínač pro ovládání osvětlení. Osvětlení na modelu představují signalizační diody umístěnými uprostřed místnosti. V rohu místnosti je instalováno čidlo PIR pro sledování pohybu v kanceláři. Toto čidlo je znázorněno jako tlačítko. Kancelář je vybavena také klimatizační jednotkou. Její stav (zapnuto/vypnuto) je určen modrou signalizační diodou.

Na modelu je také znázorněno zabezpečení oken na jednom vzorovém okně. U okna je osazeno rozpínací tlačítko, které simuluje funkci magnetického kontaktu při otevření okna. V místnosti je umístěn ještě detektor tříštění skla. Dále model obsahuje piezo sirénu, která nám simuluje sirénu při vyhlášení poplachu. Pro ovládání přístupového a zabezpečovacího systému je na modelu osazena klávesnice.

6.2 Jak model pracuje

Model kanceláře představuje přístupový a zabezpečovací systém v jednom. Prvky sloužící pro zabezpečení jsou na modelu schematicky zobrazeny. Jedná se o zabezpečení okna proti neoprávněnému otevření z vnějšku nebo násilném vniknutí rozbitím skla, zabezpečení dveří při neoprávněném vstupu nebo násilném otevření a zabezpečení prostoru kanceláře jako celku. Pro zabezpečení okna je použito detektoru tříštění skla a magnetického kontaktu (rozpínacího tlačítka). Dveře jsou zabezpečeny magnetickým kontaktem a prostor kanceláře je zabezpečen čidlem PIR na modelu reprezentovaným jako tlačítko.

Základem přístupového systému jsou přístupové body, kterými lze projít až po identifikaci a následném povolení systémem. Na modelu je znázorněn jeden přístupový bod, který je znázorněn jako dveře do místnosti. Uživatelé jsou v přístupovém systému autorizováni kartou načítanou ve snímači, který je připojen k přístupovému modulu. Jako snímač je použita čtečka karet, jak již bylo uvedeno výše. Po prověření identity a kladném vyhodnocení přístupu bude první vstupující osoba vpuštěna do střeženého prostoru kanceláře a systém provede takzvané odstřežení prostoru. Ostatní pracovníci oprávnění vstupovat do těchto prostor se musí také identifikovat čipovou kartou pro vstup do již odstřeženého prostoru. Systém si dokáže kontrolovat, kolik osob do kanceláře vstoupilo a kolik již odešlo, a to díky čtečkám karet umístěných z obou stran dveří. Z kanceláře nejde odejít bez identifikace čipovou kartou. Systém může hlídat také dvojí vstup při identifikaci jedné karty. Hlášení o tom, že se v prostoru nachází neoprávněná osoba, bude provedeno až po té, co všichni oprávnění uživatelé prostor opustí. Detektor pohybu vyhodnotí ještě před tím, něž provede zastřežení, že prostor není prázdný a zároveň nás informuje, že se v prostoru nachází neoprávněná osoba.

Systém dále dokáže vypínat osvětlení v okamžiku, kdy všichni opustí kancelář a zapomenou zhasnout osvětlení. Při opětovném příchodu se osvětlení automaticky zapne. Po zastřežení prostoru se provede vypnutí osvětlení a klimatizace. Klimatizace se nevypíná, když je kancelář prázdná, ale vždy až po zastřežení. Po odstřežení se opět sepnou výstupy klimatizace a osvětlení. Dále je řízeno vypínání klimatizační jednotky po otevření okna. Po ukončení větrání se klimatizace opět zapne. Stav okna je hlídán magnetickým kontaktem (na modelu rozpínacím kontaktem), jak již bylo

výše uvedeno. Pro řízení provozu klimatizace se předpokládá použití běžných řídících programů dle použitých jednotek. Na modelu je ukázka rozšíření tohoto řízení o již zmíněné funkce.

6.3 Prvky modelu

6.3.1 Modul ústředny

Ústředna je srdcem celého systému. Integruje v sobě zabezpečovací systém, přístupový systém a systém správy a řízení budov. Ukládá veškerá data, komunikuje s ostatními moduly a rozhoduje o další činnosti systému či některých jeho částí.

Obrázek 6: ústředna

Základní vlastnosti

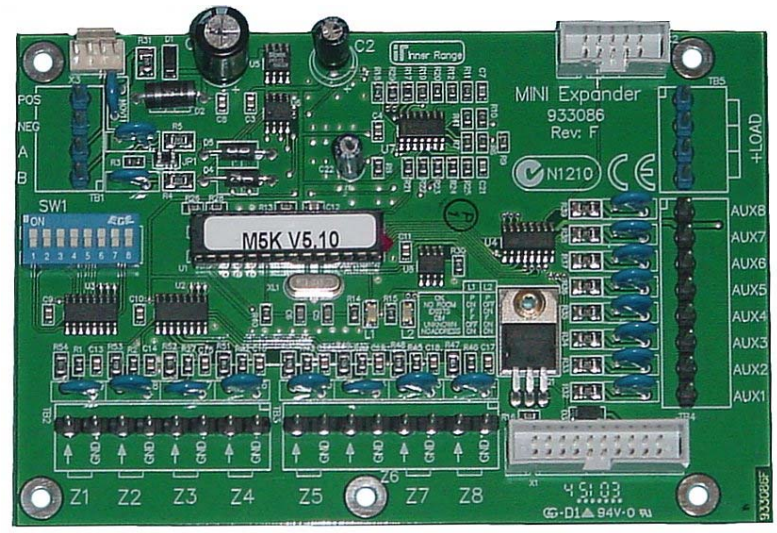
- jednotka má 16 zón přímo na desce ústředny
- jednotka má 2 výstupy s otevřeným kolektorem (max. 500 mA)
- jednotka má 2 výstupy pro modulované sirény
- na desce je osazen integrovaný telefonní komunikátor
- na desce je osazena integrovaná sériová linka (tzv. port 0)
- je možné rozšíření o další 4 sériové linky (použito u modelu)
- na desce je osazen integrovaný zdroj 3A
- systémové vstupy monitorují stav LAN, pojistek, napájení a ochranných

kontaktů modulů

• na desce jsou osazeny diagnostické LED pro snadnou identifikaci případných chyb či problémů

6.3.2 Mini Expandér

Mini expandér poskytuje rozšíření systému o osm vstupních zón a osm výstupů. U tohoto modulu lze nastavit speciální volby, jako jsou například programovatelný čas odezvy, vstupy mohou pracovat jako čítače, spínání při určitém počtu osob apod.



Obrázek 7: Mini expandér

Základní vlastnosti

• jednotka má 8 zón a 8 výstupů.

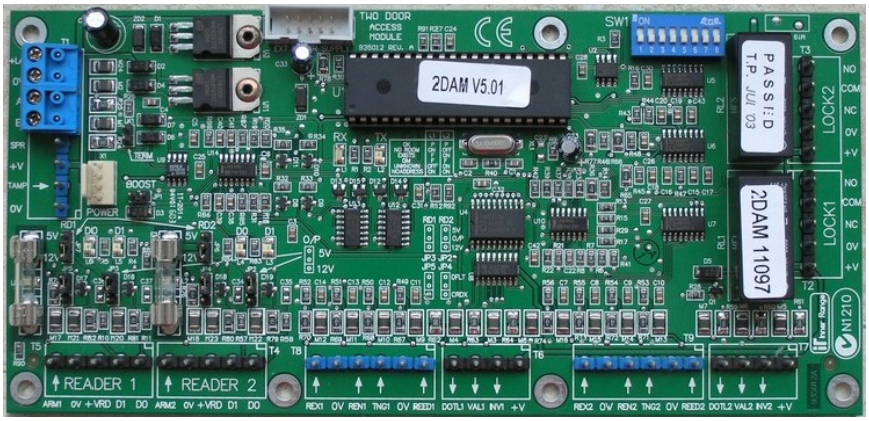
• na desce jsou osazeny diagnostické LED pro identifikaci případných chyb.

• čas odezvy vstupů je programovatelný.

• vstupy mohou pracovat jako čítače.

6.3.3 Přístupový modul

Tento modul poskytuje rozhraní pro připojení dvou čteček, které jsou využívány v přístupovém a zabezpečovacím systému a pomocí karty lze nastavovat či odstavovat jednotlivé prostory či otvírat dveře. Mezi další rozšířené funkce systému patří anti-passback, nutnost zadání dvojího kódu, průchod pouze po zadání karty i PINu, rozeznávání stavu dveří „dveře otevřeny příliš dlouho“ a „dveře násilně otevřeny“.

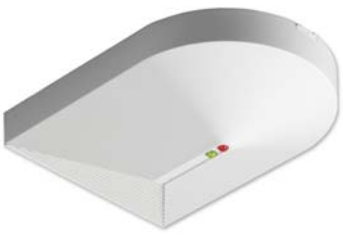


Obrázek 8: modul pro dvě čtečky

Základní vlastnosti

- jednotka pracuje v režimu 1 nebo 2 dveří (programovatelné).
- v režimu jedněch dveří dvě čtečky ovládají 1 dveře (příchodová a odchodová čtečka).
- modul obsahuje relé výstupy pro spínání zámků.
- vstupy pro monitorování stavu dveří a další zóny pro připojení jiných detektorů.
- jednotka je kompatibilní s 5V nebo 12 V čtečkami.
- záložní karty umožňují ovládat čtečku i v případě, že nelze navázat komunikaci s ústřednou.
- výstupy pro platné/neplatné karty.
- svorky pro připojení ochranného kontaktu.

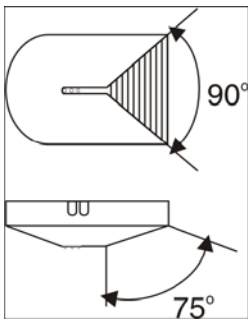
6.3.4 Tříštivý detektor skla



Obrázek 9: Detektor tříštění skla

U modelu je použit detektor tříštění skla GlassTrek (456). Tento detektor se hodí pro detekci rozbití klasických skleněných tabulí, temperovaného nebo laminovaného skla bez nutnosti dalšího komplikovaného nastavování. Čidla detekují dvě frekvence,

vniklé při porušení skla. Nízkofrekvenční vlnu nárazu a vysokou frekvenci tříštění skla. Nevzniknou-li tyto dvě frekvence současně, nedojde na čidle k vyhodnocení poplachu. GlassTrek může být použit v mnoha chráněných objektech včetně místností s okny se závěsy či zástěnami. Ve složitějších objektech lze správné vyhodnocení detektoru otestovat pomocí zařízení TestTrek. Výrobce uvádí detekce rozbití tabulí skla 40,6 x 61 cm nebo větších, pro všechny standardní tloušťky tabulí (0,3 až 0,6). GlassTrek musí být instalován na pevné ploše bez otřesů a chvění. Umístíme detektor naproti skleněným plochám, přičemž bereme v potaz detekční úhel detektoru, který je zobrazen na Obrázek 10: detekční úhel[9]. Musíme se ujistit, že strana detektoru s mikrofonem má přímý výhled na chráněné sklo a není nějak zastíněna a je v mezích detekčního úhlu.



Obrázek 10: detekční úhel[9]

Technická specifikace

- Napájení: 9 až 16 V DC
- Proudový odběr: 25 mA
- Dosah: 9 m (4.5 m)
- Rozměry: 9 cm x 6.6 cm x 2.5 cm
- Hmotnost: 100 g
- Poplachové relé: 150 mA, 28 V DC
- Tamper kontakt: 150 mA, 28 V DC
- Provozní teplota: -20°C až 50°C
- Mikroprocesor: 12/8 – bits
- Testovací přístroj: TestTrek

6.3.5 Čtečka karet

Pro kontrolu přístupu a k identifikaci osob jsou u zhotoveného modelu použity bezkontaktní karty. Pro načtení karet se používá čtečka karet HID ProxPoint Plus, která je připojena k přístupovému modulu. Zapojení čtečky k přístupovému modulu je provedeno stíněným nekrouceným kabelem. Barevné označení vodičů je uvedeno v Tabulka 1.

Tabulka 1

Funkce	Barva vodiče
+DC	červená
zem	černá
---	fialová
data 0	zelená
data 1	bílá
stínění	holý vodič
zelená LED	oranžová
červená LED	hnědá
bzučák	žlutá
hold	modrá

Test funkce

Všechny obvody čtečky se po připojení k napájení testují. Po každém připojení čtečky k napájení dojde k trojitému zablikání zelené LED a zapípání bzučáku a LED začne svítit červeně. To signalizuje, že jsou obvody čtečky v pořádku. Správné načtení karty je signalizováno přebliknutím LED z červené na zelenou a pípnutím bzučáku.

Technická specifikace

- Rozměry: 79.6 x 43.7 x 16.8 mm
- Materiál: polykarbonát UL 94
- Napájecí napětí: 5V až 12 V =

- Proudový odběr: v klidu 30 mA, špičkový 75 mA
- Provozní teplota: -30°C až 65°C
- Relativní vlhkost: 0 až 95% nekondenzační
- Přenosová frekvence: 125 kHz
- Hmotnost: 75 g
- Délka kabelu: max. 153 m (s kabelem 22 AWG)

V systému jsou použity bezkontaktní karty HID Corporation, technologie HID - PROX CARD II. Jedná se o ekonomickou variantu karet vyrobených z PVC, frekvence je 125kHz. Karta má zvýšenou odolnost proti poškození.

http://www.kelcom.cz/products/v_proxcardII.jpg

6.3.6 Klávesnice

LCD klávesnice nám na modelu slouží k nastavení a ovládání systému. Na klávesnici se zobrazují stavy systému např. zastřeženo/odstřeženo. LCD klávesnice má 20 podsvětlených kláves a podsvětlený LCD displej.
.

Obrázek 11: Klávesnice

Základní vlastnosti

- Zadní kryt klávesnice je určen pro povrchovou nebo zapuštěnou montáž
- Podsvětlený LCD display
- Instalační a uživatelské informace podporují češtinu.
- Čtyři LED mohou zobrazovat stav prostorů, funkci dveří, alarmů nebo jiných voleb - jsou volně programovatelné.

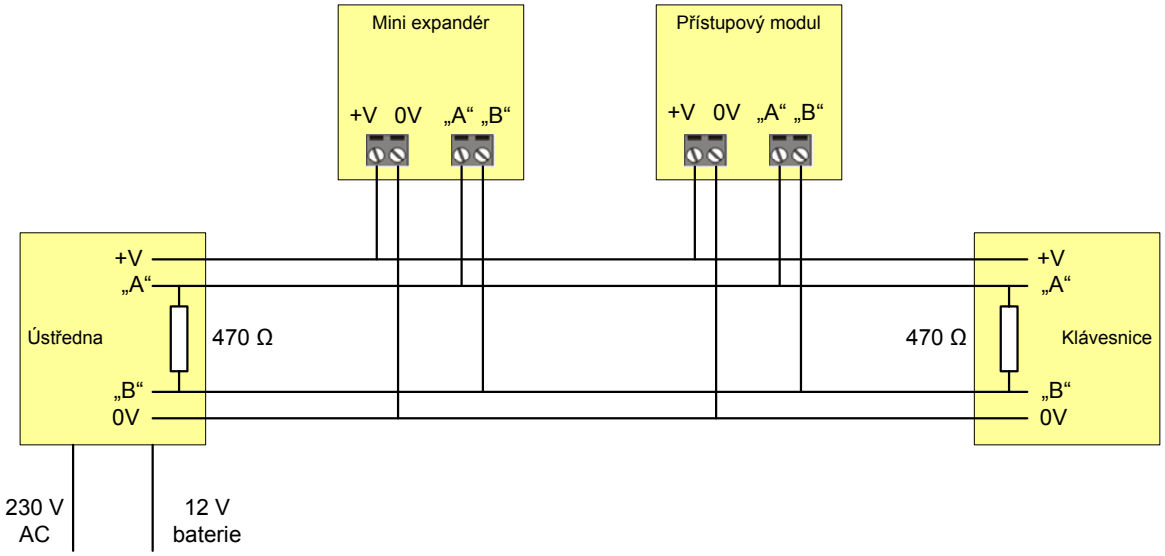
- Adresa se nastavuje přímo na klávesnici
- Programovací volby dovolují specifikovat, který prostor bude přiřazen vybrané klávesnici.
- Klávesa „HELP“ je aktivní v každém okamžiku a je schopna pomoci při běžných uživatelských úkonech.
- Čtyři klávesy šipek poskytují rychlý a výhodný přístup k programovacím volbám v tabulkovém stylu menu.
- Klávesnice poskytuje 2 vstupy a 2 výstupy.
- Je detekován a monitorován stav ochranných kontaktů
- Programovatelná „panik“ klávesa.
- Programovatelný nátlakový kód

6.4 Zapojení modelu

Zapojení modelu lze rozdělit na dvě samostatné oblasti. Jedna oblast řeší komunikaci mezi jednotkami a napájení těchto jednotek (modulů). Druhá oblast představuje funkční zapojení jednotlivých modulů.

6.4.1 Komunikace mezi moduly

Propojení ústředny s ostatními moduly je přes RS 485 krouceným párovým kabelem UTP kategorie 6 dle specifikace EN50173. Dle výrobce by postačoval kabel UTP kategorie 3. Toto propojení je znázorněno na Obrázek 12. V kabelu jsou použity čtyři vodiče. Dva vodiče jsou signály “A“ a “B“ , které jsou propojeny na všech modulech. Pro vedení těchto signálů je použit jeden pár krouceného párového kabelu. Vždy musí být oba tyto signály zapojeny na stejném páru. Další dva vodiče slouží pro napájení modulů bez vlastního zdroje. Signál “NEG“ musí být propojen na všech modulech. Signál „+V“ slouží pro napájení modulů bez vlastního zdroje. V našem případě jsou všechny moduly napájeny z ústředny. Pro dosažení optimálního výkonu a funkčnosti RS 485 je nutné na dvou nejvzdálenějších bodech sběrnice provést její zakončení. Toto se provádí pomocí ukončovacích propojek či nastavením ukončovacích DIP přepínačů. Vložením propojky či nastavením DIP přepínače dochází k „vložení“ rezistoru 470 ohmů mezi signály “A“ a “B“ jak je znázorněno na Obrázek 12: Blokové schéma zapojení modulů přes RS485.

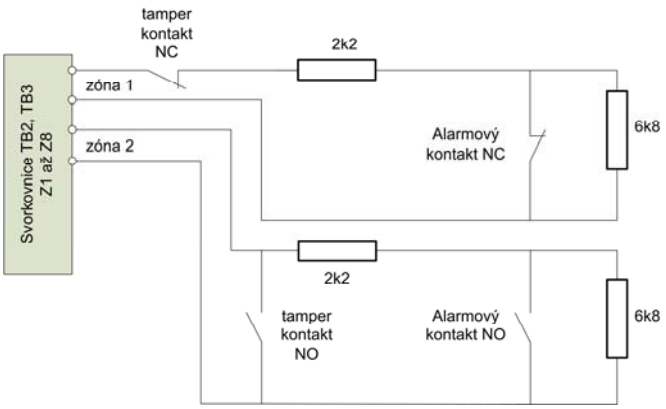


Obrázek 12: Blokové schéma zapojení modulů přes RS485

6.4.2 Zapojení jednotky mini expandéru

6.4.2.1 Zapojení zón

Na obrázku č. Obrázek 13 je znázorněno zapojení jednotlivých zón mini expandéru. Zóny se připojují k jednotce prostřednictvím svorkovnice TB2 a TB3. Na demonstračním modelu jsou k mini expandéru připojeny prvky pro sledování zastřeženého prostoru. Jedná se o magnetický kontakt, detektor tříštění skla a PIR čidlo. PIR čidlo je na modelu reprezentováno jako rozpínací tlačítko.

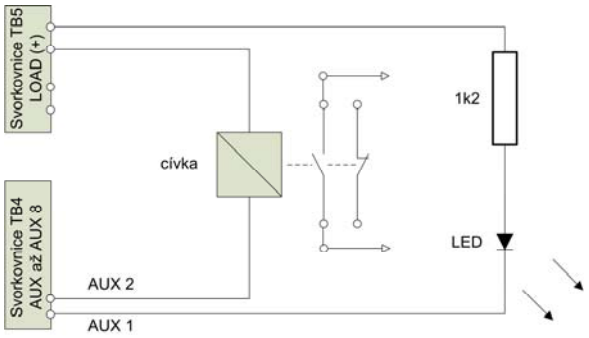


Obrázek 13: schéma zapojení zón

6.4.2.2 Zapojení výstupů - AUXů

Obrázek 14 znázorňuje zapojení jednotlivých výstupů (AUXů). V praxi musí být většinou modul napájen z externího zdroje, protože RS 485 neposkytuje dostatečný proud pro napájení auxů a detektorů. V našem případě se jedná o malé zátěže, proto jsou všechny

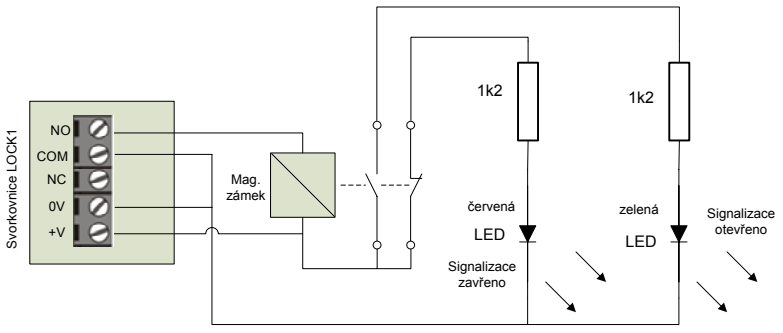
auxy a zóny napájeny z LAN. Z mini expandéru jsou připojeny výstupy ovládání klimatizace, osvětlení a výstup poplachové sirény.



Obrázek 14: schéma zapojení výstupů

6.4.3 Zapojení přístupového modulu

K přístupovému modulu jsou připojeny čtečky karet a je odtud ovládán elektrický zámek dveří. Čtečky karet ovládají jedny dveře a jsou zapojeny do jednotky podle tabulky uvedené v bodě 6.3.5 Elektrický zámek dveří je připojen na svorkovnici LOCK 1. Na modelu simuluje funkci zámku signalizační dioda umístěná u dveří. Dioda má po zapnutí modelu dva stavy svitu, červená nebo zelená. Zelená znázorňuje otevření zámků dveří a červená naopak zavřeno. Na Obrázek 15: zapojení zámků dveří se signalizací stavů je znázorněno zapojení výstupu pro ovládání zámku dveří se signalizací stavu. U modelu jsou signalizovány, jak již bylo zmíněno, pouze stavy.

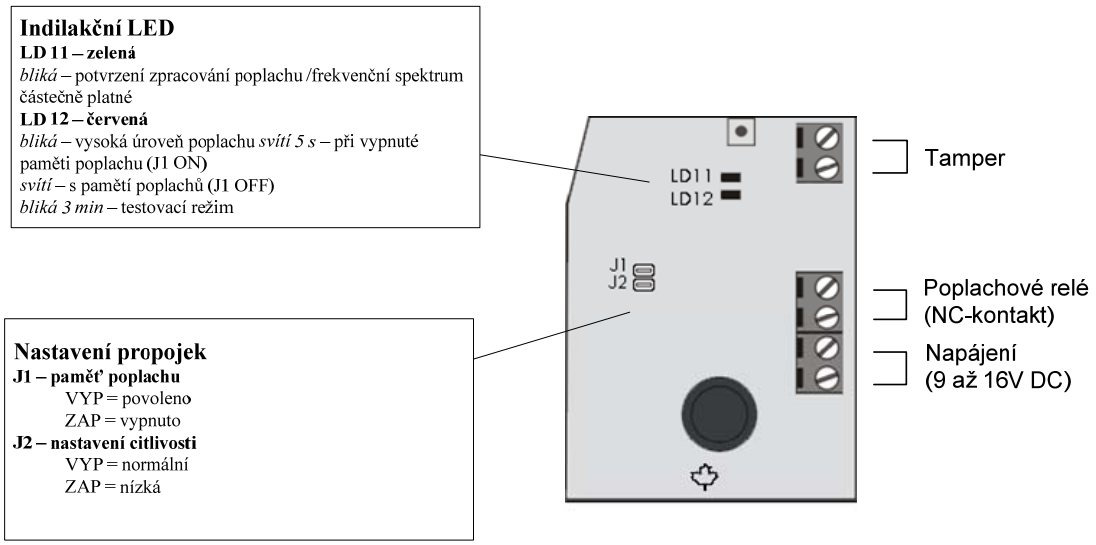


Obrázek 15: zapojení zámků dveří se signalizací stavů

6.4.4 Zapojení detektorů tříštění skla GlassTrek

Detektor je připojen k Mini expandéru. Pro připojení jsou použity čtyři vodiče, dva pro napájení a dva pro poplachový stav. Poplachové relé detektoru je připojeno na zónu Z3 v Mini expandéru. Při vyhodnocení poplachu dojde k rozepnutí poplachového relé a následně ke spuštění alarmu v případě, že je alarm aktivován.

Tamperový kontakt krytu čidla není na modelu používán. Na Obrázek 16 jsou zobrazeny svorky detektoru s popisem jejich zapojení



Obrázek 16: Zapojení detektoru GlassTrek

6.5 Možnosti rozšíření systému

Model, který je součástí této práce, má své omezení ve smyslu jak rozměrů, tak ve smyslu finančních možností. Proto se chci v této části zmínit o tom, co vše je možné v automatizaci budov automatizovat pomocí zde použitého systému CONCEPT.

6.5.1 Řízení výtahů

Systém umožňuje řídit přístup max. 32 výtahových kabin až do 64 pater. V systému lze nastavit tři druhy řízení výtahu:

a) Jednoduché ovládání pomocí výstupů bez zpětné informace o stisku tlačítka. Systém po přiložení karty sepne na určitou dobu výstupy, které „povolují“ tlačítka jednotlivých pater. Tato varianta ovládání se používá v případech, kdy není nutné mít informaci o tom, které tlačítko uživatel vybral.

b) Jednoduché ovládání pomocí vstupů a výstupů se zpětnou informací o stisku tlačítka. Systém po přiložení karty snímá po určitou dobu vybrané vstupy a po narušení konkrétního vstupu sepne korespondující výstup, pokud toto dovoluje i nastavení uživatele. Tento typ ovládání výtahu se používá v případech, kdy je nutné mít informaci o výběru patra konkrétním uživatelem.

c) Vysokoúrovňové ovládání skrze linku RS 232.

Systém předává informace o přistupujícím uživateli a vybraném patře pomocí sériové linky. Řídící systém výtahu musí podporovat komunikaci ve formátu OTIS/B.

6.5.2 Řízení klimatizace

Řízení klimatizace probíhá pomocí výstupů na základě stavu vstupů. Maximálně lze ovládat 4 klimatizační jednotky, každá klimatizační jednotka může řídit klimatizaci v max. 10 prostorech.

6.5.3 Ovládání dalších prvků

Systém Concept nezapomíná ani na řízení jednodušších elektrospotřebičů pomocí výstupů. Dále lze nastavit použití programové volby, které umožňují definici vlastní funkce určitého prvku systému (např. výstupu) na základě stavu jiného prvku (např. zóny). Tak lze definovat funkci, která umožní spínání osvětlení po detekci pohybu v určitém prostoru. Analogový modul může monitorovat a vyhodnocovat spojitě se měnící veličiny jako třeba teplotu, vlhkost půdy atd.

7 Programování modelu

Po sestavení všech prvků modelu, správném zapojení a připojení napájecího napětí systém vůbec nic neumí. Musí se tedy tento model naprogramovat tak, aby se choval podle našich požadavku, v tomto případě uvedených v bodě 6. Naprogramování je možné provést dvěma způsoby. Jedna možnost je naprogramovat systém pomocí LCD klávesnice k tomu určené. Tento způsob je poměrně zdlouhavý a méně vhodný pro nastavování složitějších požadavků. Vstup do systému pomocí LCD klávesnice za účelem programování, ale také za účelem ovládání nebo přístupu do prostor je umožněn po zadání přístupového kódu, který spočívá v zadání jednotlivých číslic PINu a následným potvrzením klávesou OK. Druhá možnost jak provést naprogramování systému je pomocí k tomu určenému softwaru přes PC. Tento druhý zmíněný postup byl použit pro naprogramování zhotoveného modelu, a to konkrétně pomocí softwaru Insight.

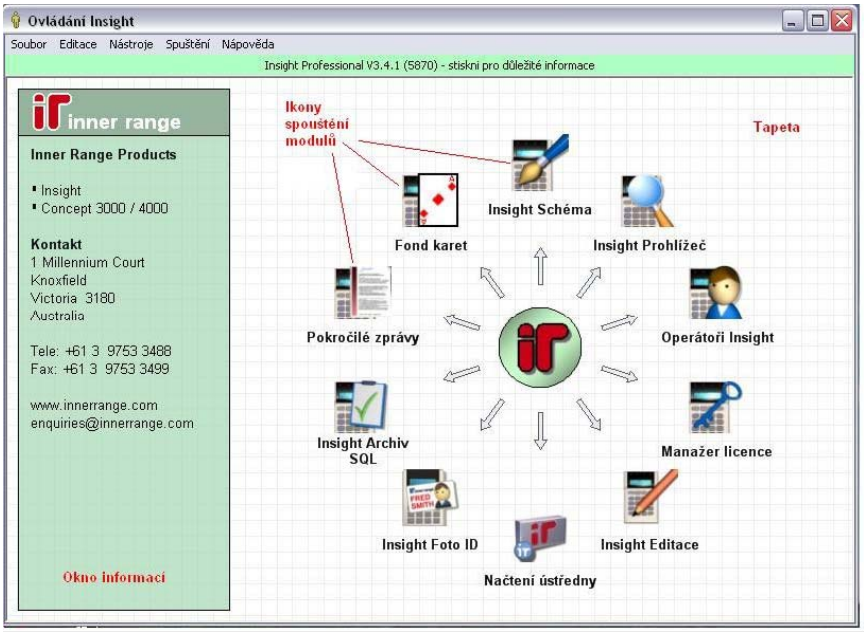
7.1 Insight

Insight je software nové generace pro správu a konfiguraci zabezpečovacích systémů Concept od firmy Inner Range. Verze Lite nabízí uživatelům poměrně rychlé nahrávání a stahování, kontrolu filtrování, kontrolu hardware a panel s nástroji pro celkové ovládání systému. Podporuje dlouhé názvy a popisky všech programovatelných položek, pokročilé vyhledávání, křížové odkazy, režim "on - line", "off - line", upravování, funkce " kopírovat " a " vložit ", automatickou detekci změn v terminálu, databázi, automatickou úpravu konfigurace paměti, stav LAN modulů, náhodnou generace PIN kódů. Insight Lite je určen pro montážní techniky k naprogramování a odladění systému, není určen pro koncové uživatele.

Insight Profesional je obchodní balíček určeny pro koncové uživatele systému. Software je postaven na kvalitní bázi Lite verze programu, a to přidáním nových modulů a dalších prvků obsažených v multi-panelu, multi-pracovní stanici a ve vnitřních zprávách. Modul operátora umožňuje udělovat a rušit oprávnění přístupů. Modul zobrazení umožňuje přidávat grafické mapy a plánky prostorů, zjištění aktuálního stavu, vložení skutečné fotografie. INSIGHT přináší zlom v technologiích pro společná bezpečnostní řešení. Tato verze softwaru přináší kompletní správu poplachů, speciální zprávy, panel multi-nájemník a virtuální multi-panel. Insight vyžaduje Windows 2000 nebo Windows XP a verzi 5 firmware ústředny.

7.1.1 Úvod do Insight

Insight se skládá z několika modulů. Každý modul představuje samostatný program pro práci s instalací systému Concept. Po spuštění se nabízí možnost otevření jednotlivých modulů Insight výběrem jejich ikon. Ovládací okno, které je zobrazeno po spuštění programu je na Obrázek 17**Chyba! Nenalezen zdroj odkazů.** Pro informaci je zde uveden popis jednotlivých modulů:



Obrázek 17: Ovládání Insight

Insight Editace (Insight Edit) program pro programování systémů Inner Range

Insight Prohlížeč (Insight Review) program pro prohlížení a archivaci událostí v systémech Inner Range

Manažér licence (Licence Manager) aktivace placených služeb (není v Insight Lite).

Fond karet (Card Pool) správa přístupových karet pro SITE kód i přímý vstup, samostatně licencovaný (není v Insight Lite).

Operátoři Insight (Insight Operator) program pro správu práv a přístupu

jednotlivých operátorů programu (není v Insight Lite).

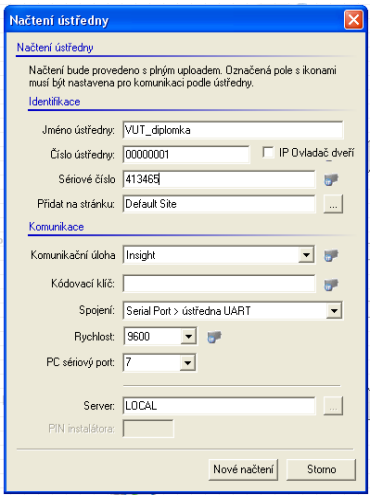
Insight Archiv SQL (Insight Archiver) program pro správu databázových dat systémů Inner Range.

Pokročilé zprávy (Advanced Reports) pro vytváření zpráv včetně jejich šablon a vzorů, samostatně licencovaný (Není v Insight Lite).

Insight Schéma (Insight Schematic) program pro monitorování stavu systému na základě intuitivního grafického zobrazení instalace systému (není v Insight Lite).

Insight ID foto (Insight Photo ID) program pro vytváření ID karet uživatel (není v Insight Lite), samostatně licencovaný.

Pro programování, prohlížení a konfiguraci jednotlivých funkcí v systému CONCEPT se používá modul *Editace Insight*. Dále se tento modul využívá pro správu uživatelů, jejich karet a PINů. Než však začneme se samotným programováním systému, musíme propojit počítač s ústřednou a poté načíst ústřednu. Možností propojení je několik. V Tabulka 2 jsou možné propojovací cesty uvedeny. Pro náš případ byla použita propojovací cesta (připojení) přes sériový port RS 232. Načtení ústředny se provádí pomocí modulu „načtení ústředny“ v *Insight*. Pro načítání ústředny je třeba znát sériové číslo ústředny, které musíme zadat při načítání. Ústředna musí být zapnuta a v Insight musí být nastaven zvolený typ komunikace. V našem případě sériový port. Na Obrázek 18 je zobrazena tabulka, do které se zadávají dané parametry.



Obrázek 18: Insight načtení ústředny

Závazné jsou zejména údaje:

- číslo ústředny - musí být zadáno vždy 8 číslic (první dvě musí být nuly)
- výrobní číslo - musí být zadáno přesně dle informací z ústředny
- komunikační úloha - musí být nastaveno Insight
- rychlost - musí být zadána stejná jako v ústředně (obvykle 9600Bd)
- server - ponechat nastavení na LOCAL

Tabulka 2

Připojení	Modul ústředny	Nastavení Insight	Typ spojení
Ethernet	Ethernet UART	TCP/IP	Stálé
Sériové	UART deska IRPX 3000EU	Sériový port	Stálé
Vytáčení	Externí/interní modem	Modem	Dočasné
GSM	GSM modul FE3000	TCP/IP	Dočasné

7.1.2 Připojení ústředny k Insight

Po načtení ústředny, které bylo zmíněno předchozím bodě, se ještě musí ústředna připojit k pc. To provedeme v programu Insight v modulu „Editace“ (Insight Edit). V přehledovém okně vyhledáme tuto ústřednu. Pravým tlačítkem klikneme na tuto ústřednu a vybereme nabídku „Automatické připojení“. Barva ústředny zezelená a začne přenos dat, číselná hodnota v závorce za jejím názvem se začne zmenšovat a následně zmizí. V tom okamžiku je přenos dat ukončen. Ještě můžeme nastavit datum a čas v ústředně, pravým tlačítkem klikneme na ústřednu a vybereme „Vlastnosti“, v hlavním okně se objeví okno s názvem ústředny, vybereme volbu „Údržba“ a zde můžeme změnit čas. Vhodná je volba poslat čas PC do ústředny.

7.1.3 Insight Editace

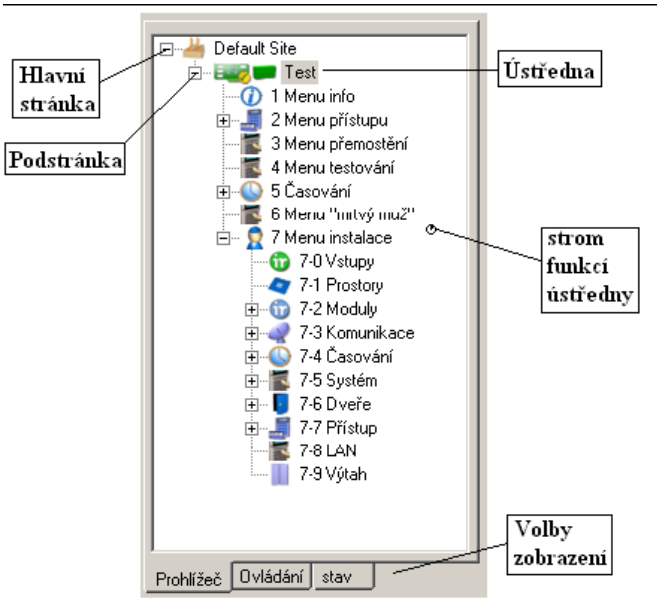
Tento modul se používá pro programování, prohlížení a definování jednotlivých funkcí systému. Programování se provádí na základě výběru funkce (moduly, uživatelé, zóny, atd.) v přehledovém okně, v pracovním okně se objeví přehled všech jednotek této funkce a kliknutím na jednu z nich se otevře editační okno této jednotky. Jestliže ústředna není při programování připojena, veškeré změny se přenesou do ústředny při nejbližším spojení PC s ústřednou. Bližší vysvětlení bude provedeno dále při popisu programování.

7.1.4 Přehledové okno Insight

Přehledové okno je řídícím centrem všech modulů Insight. Umožňuje vytvářet a spravovat stránky, načítat ústředny, ovládat periferní zařízení, programovat a provádět údržbu ústředny. Je v každém modulu Insight. Obsahuje jednu nebo několik hlavních stránek. V ní jsou vnořeny podstránky, reprezentované již názvy jednotlivých systémů (ústředen). Ty pak lze rozvinout do seznamu – stromu funkcí (modulů) ústředny, pro každou ústřednu (podstránku) samostatně. Spodní tři záložky

přepínají volby zobrazení:

- Prohlížeč (detailní zobrazení podstránek a všech jejich funkcí),
- Ovládání (detailní zobrazení podstránek a funkcí umožňujících ovládání),
- Stav (souhrnné zobrazení podstránek-ústředen a jejich stavu).



Obrázek 19: přehledové okno Insight

7.2 Nastavení systému

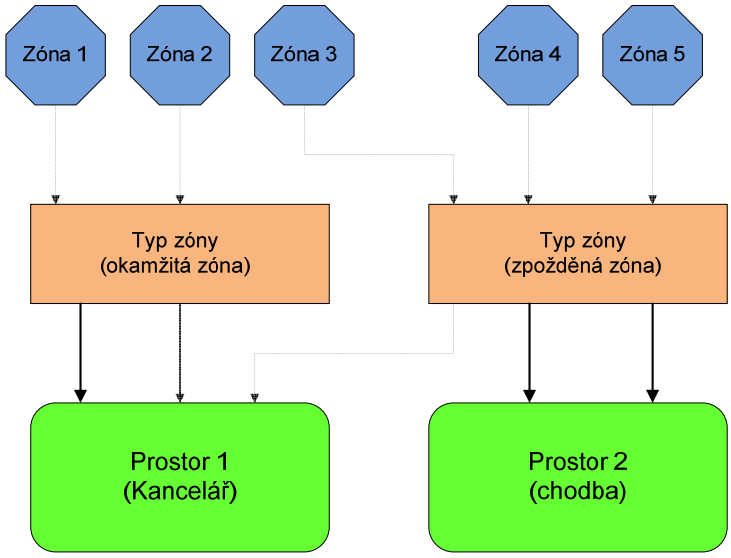
Jak už bylo zmíněno, systém CONCEPT se programuje pomocí softwaru Insightu. Používá se k tomu konkrétně programový modul „Insight Editace“. Pro lepší představu programovací struktury si rozdělíme systém na tři základní body – zabezpečovací systém, správa uživatelů a přístupový systém. Zde si ukážeme pomocí blokových schémat princip programování.

7.2.1 Základní princip

7.2.1.1 Zabezpečovací systém

Programové volby zabezpečovacího systému se dají rozdělit na jednotlivé zóny, pro které lze nastavit základní parametry jako jsou jméno, typ detektoru se spínacími (N.O.) nebo rozpínacími (N.C.) kontakty. Tyto zóny se seskupují do vyšších celků (prostorů), kterým se dají nastavit další volby, které se již netýkají přímo zón (volby sirén, výstupů, atd.). Každá zóna je přiřazena do skupiny nazvané typy zóny, které určují základní „chování“ použitých zón – např. stavy, na které bude systém reagovat, nastavení komunikačních kódů, nastavení spínání sirén, konfigurace zobrazení zpráv na LCD klávesnicích, atd. Typ zóny je takzvaně prostředník mezi zónami a

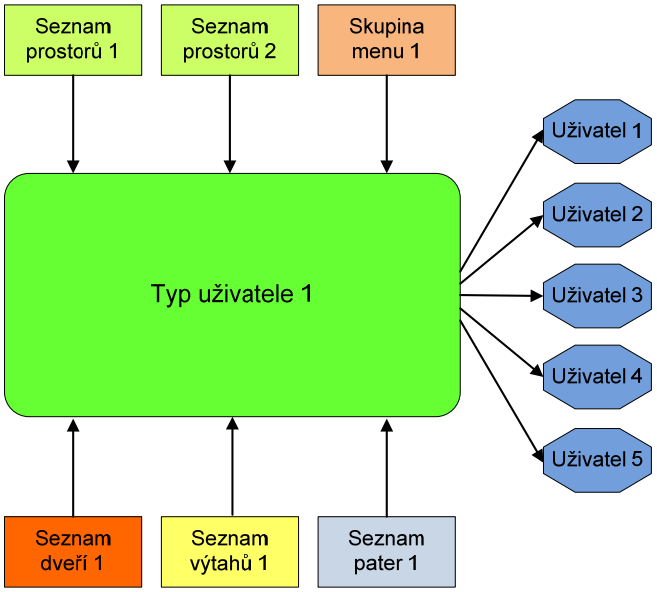
prostorem.



Obrázek 20: Základní schéma programových voleb zabezpečení

7.2.1.2 Správa uživatelů

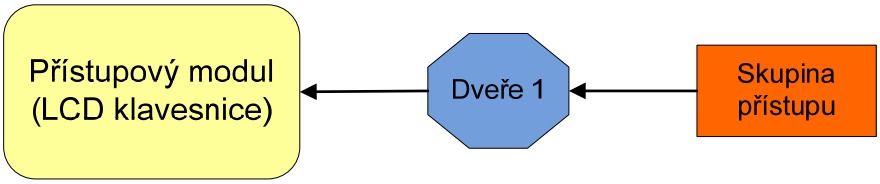
Každý uživatel má přidělena svá uživatelská práva. Uživatelská práva (např. právo ovládat určitý prostor) se v systému Concept nezadávají přímo konkrétnímu uživateli, ale obvykle „skupině“ (profilu), které říkáme typ uživatele. Tato metoda přiřazování „uživatelských“ práv má své opodstatnění při vyšším počtu uživatelů, dosáhneme tak vyšší rychlosti celkového nastavení všech uživatelů, ale také menší spotřebu „systémových zdrojů“. Mezi základní „uživatelská“ nastavení patří určení prostorů, které bude mít uživatel (resp. uživatelé daného typu) možnost ovládat, dále určení povolených funkcí v systému a výčet dveří s povoleným průchodem. Tato nastavení se opět nepřiřazují přímo, ale pomocí tzv. seznamů, které obsahují výčet použitých prvků (např. seznam prostorů určuje, které prostory smí daný typ uživatele používat). Na obrázku 21 je tento princip schematicky znázorněn.



Obrázek 21: Základní schéma uživatelských programových voleb

7.2.1.3 Přístupový systém

Základním prvkem přístupového systému jsou dveře. Jednotlivým dveřím lze nastavit řadu individuálních voleb (jméno, výstup zámku dveří, doba sepnutí zámku, doba otevření dveří, atd.). Další volby, které již nemusejí být definovány specificky pro jednotlivé dveře, jsou tzv. „skupiny přístupu“. Tyto skupiny přístupu určují zejména prostředky, kterými lze získat přístup ke dveřím (např. LCD klávesnice, přístupové moduly) a dále „provázání“ přístupového a zabezpečovacího systému. Posledním krokem při vytváření přístupového systému je přiřazení vytvořených dveří některému z modulů (konkrétní LCD klávesnici či přístupovému modulu).



Obrázek 22: Základní schéma programových voleb

7.2.2 Zadaní uživatelů do systému

U nového systému, nastaveného na tovární hodnoty, jsou vytvořeni dva uživatelé, uživatel 00001 – TECHNIK (U00001) a uživatel 00002 - MASTER (U00002). Označení (U00001) je instalační kód se zvláštními pravomocemi a označení (U00002) je master kód, který má specifické funkce v systému.

U00001 – TECHNIK má PIN standardně nastaven na 01. Má oprávnění vstupovat do instalačního menu, dále má nejvyšší práva voleb v nabídkách přístupu, časování a

servisního menu a také má umožněn dálkový přístup v závislosti na nastavení dálkového přístupu ve skupinách menu (přístup může být zakázán uživatelem U00002 – MASTER).

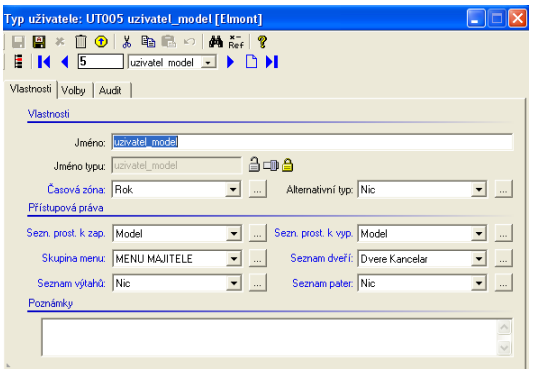
U00002 – MASTER má PIN standardně nastaven na 02. Má oprávnění k programování ostatních uživatelů (mimo U00001), má umožněn dálkový přístup v závislosti na nastavení dálkového přístupu ve skupinách menu, může zakázat přístup do systému U00001 – technikovi. Nejčastěji je U00002 přidělován majiteli systému nebo pracovníkovi odpovědnému za zabezpečení systému.

U00003 je již standardní uživatel s výjimkou práv dálkového přístupu, která se nastavují stejně jako u U00001 a U00002. Pokud uživatelův "Typ" (typ uživatele) umožňuje změnu ostatních uživatelských kódů (specifikováno ve „skupině menu“), potom je uživateli umožněno změnit pouze uživatele s pořadovým číslem, které je rovné nebo vyšší než je jeho vlastní.

Uživatelé přiřazeni u modelu jsou charakterizováni:

- Typem uživatele
- PINEM uživatele
- Kartou uživatele
- Jménem uživatele

Ještě než přidáme jednotlivé uživatele do systému, musíme nadefinovat jednotlivé typy uživatelů. Toto se provádí v menu 2.2. Typ uživatele určuje každému uživateli jeho práva k ovládání systému (přístup, prostory, atd.). Každý uživatel musí mít přiřazen typ uživatele. Uživatel bez přiřazeného typu uživatele nemá žádná práva k systému. Podle velikosti a konfigurace paměti může být programováno až 250 typů uživatelů.



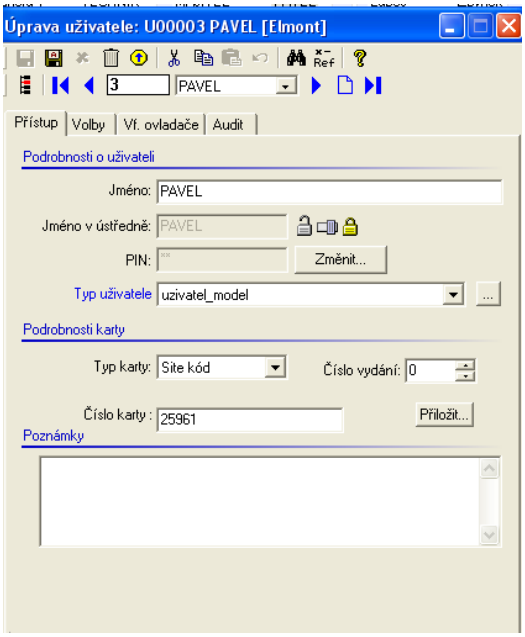
Obrázek 23: Insight zadání typu uživatele

V menu 2.2 se definuje seznam prostorů k zapnutí, seznam prostorů k vypnutí, skupina menu, seznam dveří a další pro náš případ již nedůležité položky.

Seznam prostorů k zapnutí je pole pro volbu seznamu prostorů, které může tento typ uživatele zapnout. Seznam prostorů k vypnutí je pole pro volbu seznamu prostorů,

které může tento typ uživatele vypnout. Není-li přiřazen žádný seznam prostorů k zapnutí či vypnutí, nemůže tento typ uživatele žádné prostory zapnout či vypnout. Skupina menu je pole pro volbu skupiny menu přiřazené typu uživatele. Skupina menu definuje operace, které může tento typ uživatele provádět z LCD klávesnice. Skupina dveří je pole pro volbu seznamu dveří, které může tento typ uživatele použít pro příchod/odchod. Není-li přiřazen žádný seznam dveří, nemůže typ uživatele žádné dveře použít. Při programování modelu byly nastaveny následující parametry:

- pole seznam prostorů k zapnutí: model
- pole seznam prostorů k vypnutí: model
- pole skupina menu: menu majitele, menu zaměstnance
- pole seznam dveří: dveře kancelář



Obrázek 24: Insight zadání uživatele

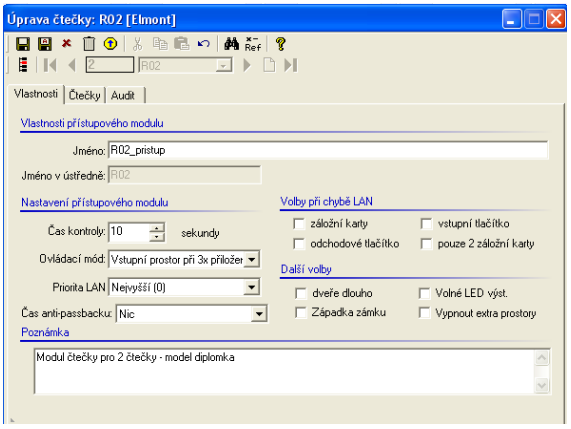
Přidání uživatelů do systému se provede v Insight Edit menu 2.1. V modelu jsou načteny pro testování modelu čtyři uživatelé. U každého uživatele musí být zadán typ uživatele. V našem případě je to „uživatel_model“ jak je vidět na Obrázek 24: Insight zadání uživatele. Dále má každý uživatel zadán svůj PIN a je zde definován typ a číslo karty. Pro testování modelu budeme používat bezkontaktní karty HID se čtečkami ve formátu Wiegand. Proto je zadáno v poli typ karty „Site karta“, která se používá u karet se site kódem. Site kód je část čísla karty, který je společný pro všechny karty na dané instalaci. Číslo karty je číslo, které je uvedeno na každé použité kartě. Dále musíme nastavit v záložce volby extra prostor, do kterého má daný uživatel právo vstoupit, zapnout či vypnout zastřežení.

7.2.3 Zadání ostatních parametrů

Než začneme programovat zabezpečovací a přístupový systém, musíme v systému definovat ještě další důležité položky. Jedná se o definici seznamu prostor a seznamu dveří. Seznamy prostor jsou programovou jednotkou určenou primárně pro ovládání uživateli (zapnutí/vypnutí) více prostorů současně. Mohou být ovládány i jinými funkcemi systému Concept, např. časovou zónou, logickými auxy, domácími auxy. V závislosti na velikosti a konfiguraci paměti ústředny může být v systému až 250 seznamů prostorů. My jsme si nadefinovali prostor, který jsme pojmenovali „model“. Seznam dveří je programová jednotka, která se standardně používá pro ovládání přístupu do více dveří současně, může být použit i pro zamykání/odmykání více dveří apod. V systému může být v závislosti na velikosti a konfiguraci paměti až 250 seznamů dveří. Model má pouze jedny dveře v systému definované jako „dveře kancelář“. Ostatní seznamy použité v programu Insight tu nebudeme rozebírat, protože při programování modelu nejsou využity.

7.2.4 Programování přístupového systému

Po té, co jsme si nadefinovali seznam uživatelů, typy uživatelů, seznam prostor a seznam dveří, můžeme přejít k programování přístupu. Budeme řešit přístup do jedné kanceláře přes jedny dveře a pohyb na chodbě. Při zjištění pohybu na chodbě musí dojít v určitém čase buď ke vstupu do místnosti, nebo musí osoba opustit prostor. Toto bude podrobněji řešeno v bodě 7.2.5. V tuto chvíli se budeme zabývat tím, jak se provede nastavení systému pro přístup již nadefinovaných osob. Nejprve provedeme nastavení přístupového modulu přesněji modulu čtečky v menu 7.2.4. Toto menu slouží k naprogramovaní základních vlastností a voleb přístupového modulu (pro 1 nebo 2 čtečky) a klávesnice.

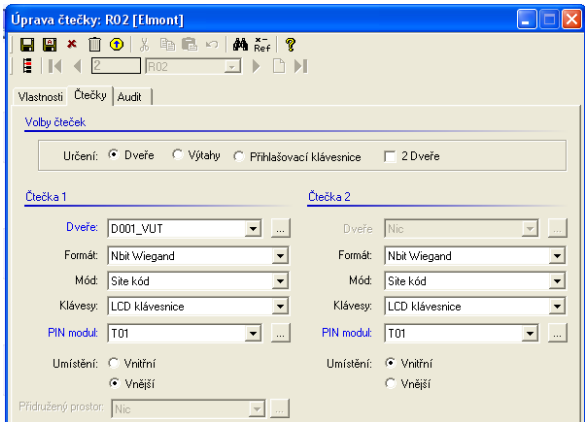


Obrázek 25: Insight vlastnosti modulu čtečky

U našeho modelu jsou použity dvě čtečky. Jedna vnější pro vstup do prostoru a druhá vnitřní pro opuštění místnosti a pro kontrolu, zda se ještě nachází někdo

v místnosti.

V menu 7.2.4 jsme kromě názvu čtečky nastavili pole ovládací mód v záložce „vlastnosti“ (vstupní prostor při 3x přiložení karty) a v záložce „čtečky“ jsme nastavili volbu čteček (čtečku jsme přiřadili dveřím), formát a mód čtečky, použitý typ klávesnice a také zvolíme klávesnici, na které se bude zadávat PIN. Ještě jsme v tomto menu provedli rozdělení vnitřní a vnější čtečky. Vše je vidět na Obrázek 25 a Obrázek 26.

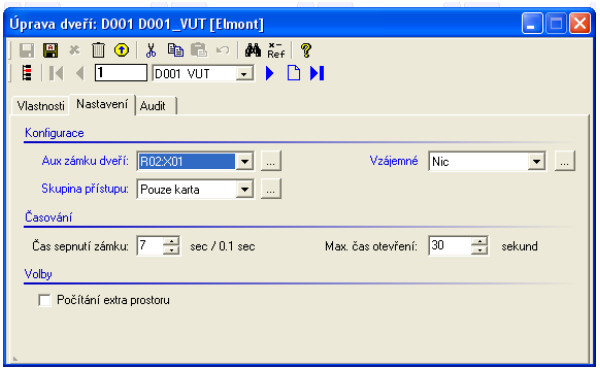


Obrázek 26: Insight nastavení čtečky

Některé volby z tabulky na Obrázek 26 popíšeme podrobněji.

- Dveře – v tomto poli byly vybrány dveře přiřazeny dvěma čtečkám. Dveře jsou vybírány podle jména/čísla, programování dveří je v Menu 7.6.1.
- Formát – zde byl vybrán formát (Wiegand) dat karty/čtečky.
- Mód – pole pro určení jakým způsobem bude karta zpracována a který uživatel bude moci tuto čtečku použít. Zde nastavíme Site kód, což lze použít pro formát Wiegand, kde je známo umístění dat Site kódu a čísla karty.

Dále provedeme naprogramování dveří v menu 7.6.1. Zadáme jméno pro lepší orientaci na klávesnici. Vybereme „vnitřní“ prostor dveří. Tento prostor může být zabezpečen při zabezpečení dveří. Vybereme „vnější“ prostor dveří. Je to prostor, který není zabezpečován.



Obrázek 27: Insight nastavení dveří

Přidružení prostoru dveřím umožní:

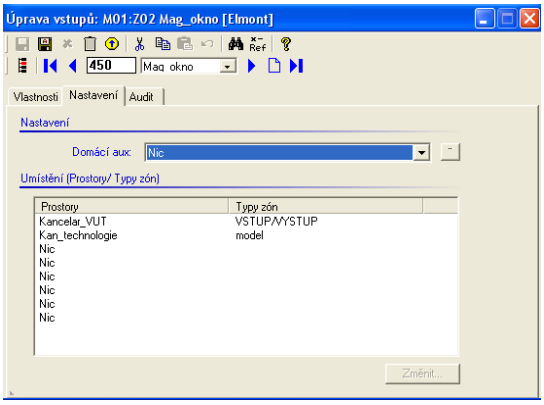
- používat pravidla antipassbacku,
- sledovat pohyb uživatele, kde se právě nachází,
- zabránit příchodu/odchodu je-li prostor zabezpečen,
- automaticky vypínat zabezpečení prostorů, je-li to povoleno
- automaticky zapínat zabezpečení prostorů při odchodu, je-li to povoleno.

Dále nastavíme správný aux zámku dveří. V našem případě jsme použili přístupový modul R02:X01. Vybereme skupinu přístupu, která bude asociována ke dveřím. Nastavíme čas sepnutí zámku. Tento čas se nastavuje ve vteřinových intervalech v rozsahu 0 až 255 sec. Při hodnotě 0 nebudou dveře znovu uzamčeny. Dveře musí být zamčeny jinou operací. Čas sepnutí zámku není závislý na časovači auxu vybraného pro ovládání zámku. Je to pouze čas použitý pro operaci otevření zámku. Můžeme ještě nastavit maximální čas otevření dveří před spuštěním poplachu, ale to na modelu nebudeme používat. Nakonec zaškrtneme volbu počítání uživatelů v „extra“ prostoru.

7.2.5 Programování zabezpečovacího systému

Zabezpečení modelu místnosti je řešeno z velké části modulem Mini expandér. Na tento modul jsou napojena všechna čidla pro střežení prostoru. Podrobněji je toto napojení popsáno v bodě 6.4.2. Přístupový modul nám slouží v tomto případě k ovládání zabezpečení, a to konkrétně k zastřežení či odstřežení prostoru. Nastavení přístupového modulu je řešeno v bodě 7.2.4. Naprogramování systému pro střežení prostoru provádíme dle blokového schématu uvedeného v bodě 7.2.1.1.

První krok je zadat systému informaci o tom, na které zóně má jednotka připojen určitý snímač. U modelu je použito pro střežení pět snímačů. Nastavení a pojmenování těchto snímačů se provádí v menu 7.0. V tomto menu se provede také přiřazení zóny danému prostoru a nastavení typu zóny. Na Obrázek 28 je vidět okno pro nastavení vstupu mini expandéru.



Obrázek 28: Insight nastavení zón

Zóny jsou do systému nastaveny podle následující tabulky:

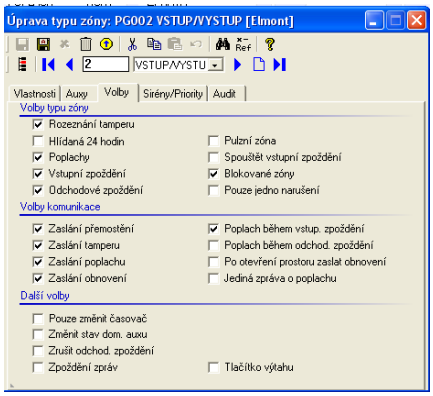
Tabulka 3

Poř. číslo	Název zón	Přiřazené čidlo	Přiřazený prostor	Typ zón
1.	M01:Z01	PIR čidlo - kancelář	Kancelář_VUT	Vstup/výstup
2.	M01:Z02	Magnetický kontakt - okno	Kancelář_VUT Kan_technologie	Vstup/výstup Model
3.	M01:Z03	Detektor tříštění skla	Kancelář_VUT	Vstup/výstup
4.	M01:Z04	PIR čidlo - kancelář	chodba	Vstup/výstup
5.	M01:Z05	Magnetický kontakt - dveře	Kancelář_VUT Chodba	Vstup/výstup Odchodová

Každá jednotlivá zóna či systémový vstup, programovaný v prostoru, musí mít přiřazen typ zóny, který určuje, jak bude zóna zpracována v tomto prostoru. Typ zón se nastavuje v menu 2.4.3. Typ zóny určuje především, které stavy vstupů budou monitorovány a zpracovávány, o kterých stavech vstupů budou zasílány zprávy, které kódy událostí a typy zpráv budou použity, které auxy prostorů budou řízeny, jak budou spínány modulované sirény a jakým tónem, jaké poplachové zprávy budou generovány pro zobrazení na displeji klávesnice, volby ovládání domácího auxu, speciální volby pro časovače auxů, zda bude poplachový stav zóny zpracováván při vypnutém prostoru a mnoho dalších voleb v našem modelu nepoužívaných.

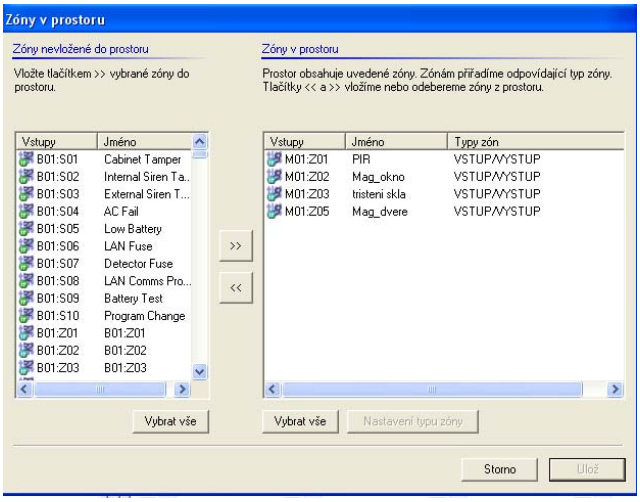
Nastavení typu zóny je druhý krok, který musíme provést pro správné nastavení systému zabezpečení. U našeho modelu je nastavena reakce zón po zastřežení prostoru. Výjimkou je zóna „model“, kde je v tomto případě nastavená reakce čidla (magnetický kontakt – okno) stále i při vypnutém prostoru. Toto nastavení je použito z důvodu ovládání klimatizace po otevření okna. Nastavení typu zóny je pro ilustraci

vidět na Obrázek 29.



Obrázek 29: Insight typ zóny

Třetí krok pro natavení zabezpečovacího systému je nastavení prostoru. To se provádí v menu 7.1. Prostory představují základní prvek ovládání bezpečnostního systému. Jsou to skupiny vstupů, na které jsou připojeny detektory, které mohou být zapnutím/vypnutím prostoru aktivovány/deaktivovány. Systém určuje, které prostory a v jaký čas může uživatel ovládat. Na Obrázek 30 je znázorněno přiřazování jednotlivých zón do prostoru. Toto přiřazování se provádí v menu 7.1 záložce „obecné“.



Obrázek 30: Insight zóny v prostoru

Dále jsme zde provedli výběr výstupu pro alarm sirény s nastavením času aktivace, nastavení příchodového a odchodového zpoždění, nastavení ovládání osvětlení při opuštění místnosti a také vypínání technologie v tomto případě klimatizace po zastřežení prostoru.

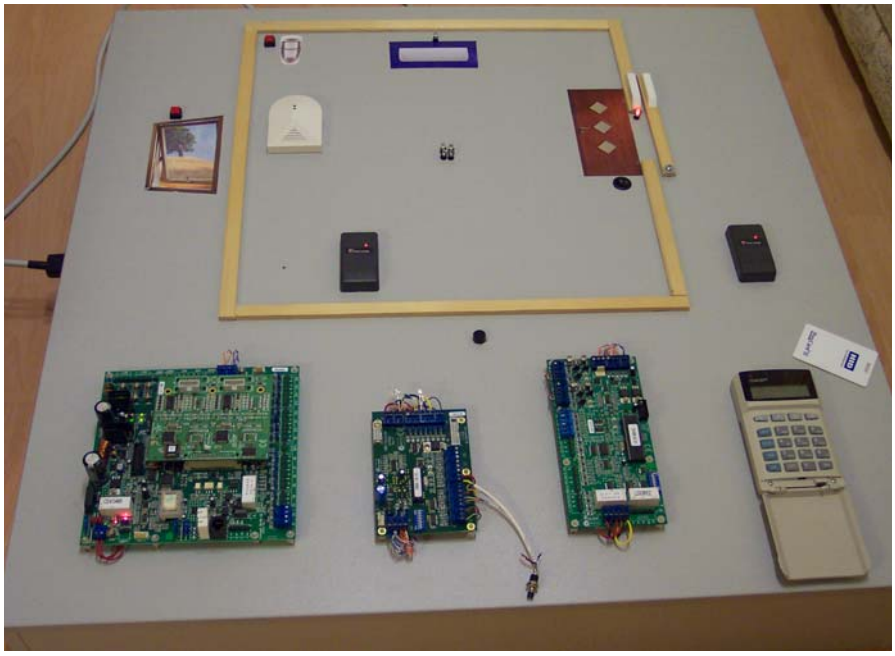
8 Prezentace modelu

V této kapitole jsou blíže prezentovány vytýčené cíle funkčnosti modelu. V kapitole 6.2 je stručný popis toho, jak má sestavený model fungovat. Zde si formou obrázku ukážeme, že model pracuje tak, jak je v této práci popsáno. Při stručném shrnutí budeme prezentovat:

- Schopnost zabezpečit systém modelu
- Přístup pomocí karet do prostoru
- Při opuštění prostoru vypnutí osvětlení
- Po otevření okna vypnutí klimatizace
- Po zabezpečení prostoru vypnutí osvětlení i klimatizace
- Po odstřežení opětovné zapnutí klimatizace a osvětlení

Další nastavené funkce systému (modelu) budou předvedeny na sestaveném modelu z důvodu nepraktičnosti prezentace touto formou obrázků. Jedná se například o zpuštění poplachu po narušení prostoru, funkci antipassback, temperový stav po zkratování nebo přerušení vedení a další.

8.1 Zabezpečení modelu



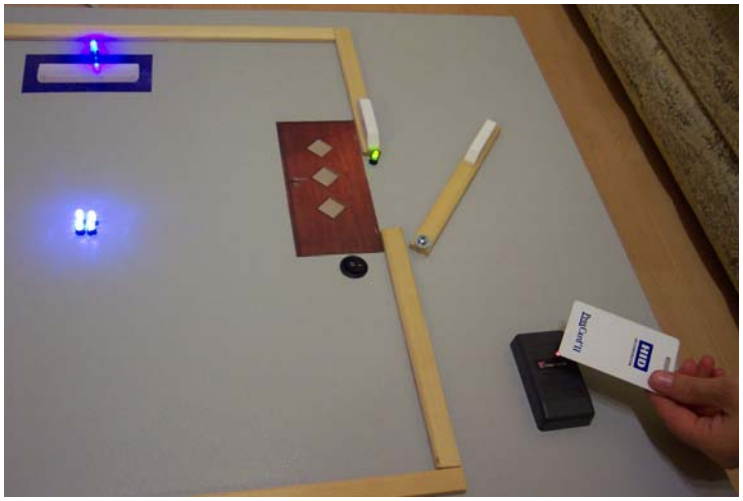
Obrázek 31: model po zabezpečení

Zabezpečení modelu se provede po 3x přiložení bezkontaktní karty k vnější čtečce karet. Následně poté se odpočítává čas pro opuštění prostoru. Na modelu je tento čas 3s. Na klávesnici je zpráva o zapnutí střežení v definovaném prostoru (kancelář VUT). Zároveň se na klávesnici rozsvítí signalizační dioda, která nás informuje o zastřežení tohoto prostoru. Na Obrázek 31 je vidět, že po zastřežení prostoru je vypnuto osvětlení a klimatizace, což je jeden z vytyčených cílů této práce.

Obrázek 32: klávesnice po zabezpečení

8.2 Přístup do prostoru pomocí karet

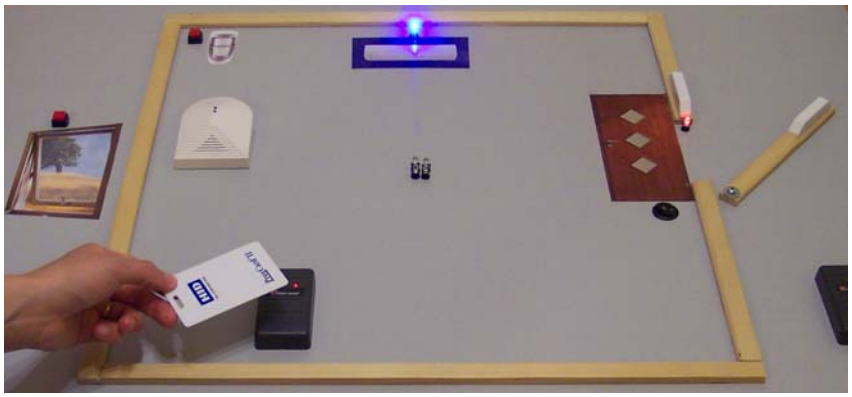
U modelu jsou nastaveni čtyři uživatelé systému, kteří mají oprávnění vstupovat do prostoru kanceláře na prezentovaném modelu. Každý z těchto uživatelů má přiřazenou bezkontaktní kartu pro identifikaci v systému. Po přiložení této karty ke čtečce karet dojde po ověření uživatele k uvolnění zámku dveří a uživatel muže vstoupit do místnosti nebo naopak opustit místnost.



Obrázek 33:Přístup pomocí karty

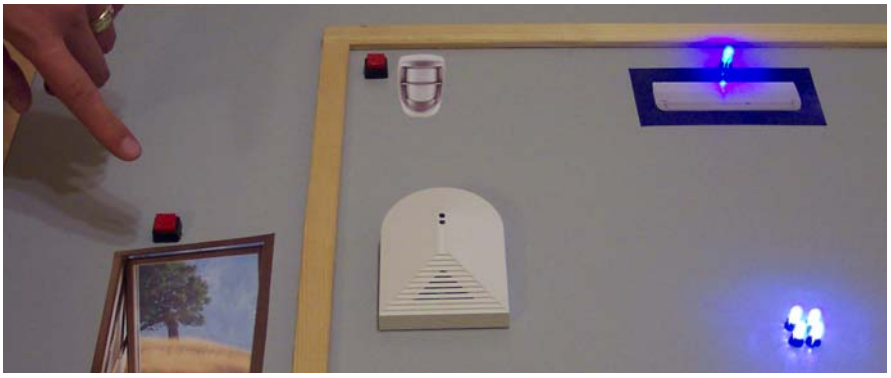
Funkce zámku je na modelu simulována, jak již bylo zmíněno, signalizační diodou. Uvolnění zámku dveří pro otevření je signalizováno zeleně svítící diodou. Naopak červeně svítící dioda simuluje zajištěný stav zámku.

8.3 Ovládání technologie modelu



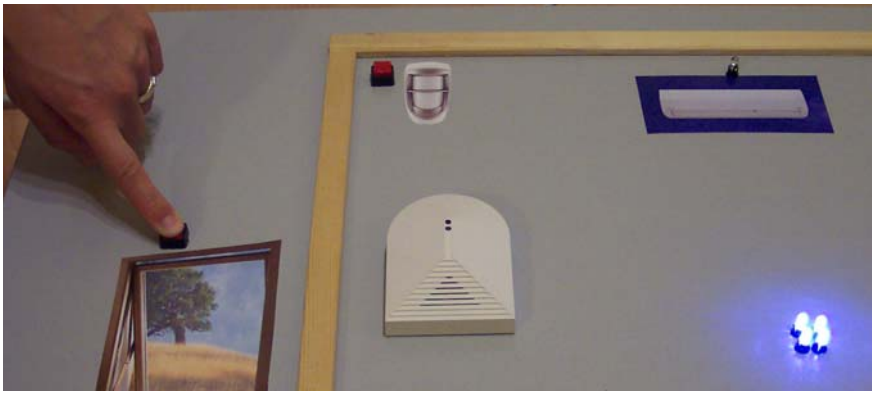
Obrázek 34: Vypnutí osvětlení při odchodu

Na modelu je prezentována příklad ovládání inteligentních budov na klimatizaci a osvětlení. Při opuštění místnosti všemi uživateli dojde automaticky k vypnutí osvětlení v případě, že tak nebylo učiněno při odchodu poslední osoby. Na Obrázek 34 je toto vypnutí znázorněno. K vypnutí klimatizace dojde automaticky až po zastřežení prostoru, což je znázorněno na Obrázek 31. Samozřejmostí je, že při příchodu první osoby do prostoru se opět aktivují všechny vypnuté výstupy (osvětlení a klimatizace).



Obrázek 35: ovládání klimatizace - okno zavřeno

Osvětlení lze dále ovládat pomocí vypínače umístěného v prostoru. U klimatizace se uvažuje další ovládání běžnými ovládacími prvky dle použité klimatizace. To již není v této práci řešeno. Na modelu je také předvedeno ovládání klimatizace po otevření okna. Otevření okna je simulováno sepnutím spínače u okna (mag. kontakt).



Obrázek 36: ovládání klimatizace - okno otevřeno

V této kapitole byly prezentovány cíle této práce na sestaveném modelu. Model byl po sestavení a naprogramování odzkoušen a výsledky fungujícího modelu zde byli stručně prezentovány. Tento model bude nadále sloužit pro testování a výuku pracovníkům firmy ELMONT GROUP a.s.. Tato firma si tento model nechal sestavit při příležitosti této diplomové práce.

9 Závěr

Tato práce se zabývá problematikou automatizace budov. Zmiňuje počátky a vývoj automatizace i nové trendy v oblasti nevýrobní automatizace, mezi něž automatizace budov patří. V práci jsou uvedeny možnosti automatizace v dnešních inteligentních budovách. Některé technologické systémy jsou rozebrány podrobněji. Práce řeší problematika ochrany majetku a ochrany budov a předpisy související s touto problematikou. Práce se podrobně zmiňuje o problematice automatizace budov u zabezpečovacích a přístupových systémů. Uvádí základní pravidla těchto systémů a postup při realizaci přístupových a zabezpečovacích systémů.

Cílem práce bylo navrhnout přístupový a zabezpečovací systém s praktickou realizací na konkrétním modelu. Byl sestaven model místnosti, na kterém je předvedeno praktické řešení této problematiky. Diplomová práce uvádí pravidla pro nastavení a programování přístupových a zabezpečovacích systémů a v samostatné kapitole pak představuje konkrétní naprogramování sestaveného modelu. Dále je na modelu předvedena možnost propojení použitého zabezpečovacího a přístupového systému s technikou řízení budov. Při sestavování modelu byl použit systém Concept od firmy Inner Range. Na trhu je mnoho systémů zabývající se přístupovými a zabezpečovacími systémy. Systém Concept požadovala použít pro sestavení modelu firma ELMONT GROUP a.s.. Této firmě bude model sloužit k prezentacím a jako výukový model pro zaškolování nových techniků. Uvedená firma zároveň hradila veškeré náklady spojené se sestavením modelu.

Systém Concept patří mezi oblíbené a často používané zabezpečovací a přístupové systémy, zejména u velmi rozsáhlých instalací. Tento systém vyniká zejména možností použití velkého počtu prostorů a také uživatelů. S tím souvisí i dostatečný počet zón pro získávání informací o systému.

Jak již bylo výše řečeno, sestavený model prezentuje přístupový a zabezpečovací systém. Zabezpečení je tu řešeno pomocí čidel umístěných uvnitř místnosti a na přístupových bodech do místnosti. Přístup je řešen pomocí přístupových karet, kde po identifikaci karty bude umožněn přístup osoby do prostoru. Systém si kontroluje počet osob vstupujících do místnosti a na základě těchto informací dokáže ovládat další prvky, v tomto případě osvětlení místnosti. Dále je na modelu předvedeno ovládání technologie budovy. Systém po zastřežení prostoru vypíná klimatizaci i osvětlení. Na modelu je také předvedeno ovládání jednotek v návaznosti na daném stavu budovy. Zde například při otevření okna se vypíná klimatizace. Z důvodů omezených finančních možností nebylo možné předvést další schopnosti systému. V případě větších finančních prostředků by bylo možné na modelu předvést další funkce jako například řízení a zabezpečení výtahů, automatické řízení klimatizace a topení, nebo také řízení jednodušších elektrospotřebičů. Další unikátní schopnost systému, která na modelu není předvedena, je snímání a vyhodnocování analogových veličin (např. teplota, intenzita osvětlení, vlhkost).

Bližší informace o sestaveném modelu, který je součástí této práce se dozvíte v kapitole 6. Programování tohoto modelu je řešeno v kapitole 7 a dosažené výsledky

splňující vytýčené cíle této práce jsou popsány v kapitole 8. Sestavený model bude nadále sloužit firmě ELMONT GROUP a.s., k prezentačním účelům a zároveň jako výukový model pro zaškolování nových techniků.

Seznam použité literatury

[1] POLIŠČUK, Radek.: Titulní strana závěrečné práce.

[2] POLIŠČUK, Radek.: Instrukce pro autory závěrečných prací, 2008, Dostupný z: http://autnt.fme.vutbr.cz/doc/SZZ2008_Instrukce.pdf.

[3] LACKO, B.; HOLÝ, M. Studijní opora magisterského studia předmětu Integrovaná nevýrobní automatizace [online]. [cit. 2009-02-20]. Dostupný z: <http://autnt.fme.vutbr.cz/lab/a4-603/opory/VIN.pdf>.

[4] SYNEK, Václav. Inteligentní budovy - současnost i historie. Konstrukce [online]. 2005 [cit. 2009-02-21]. Dostupný z: <http://www.konstrukce.cz/clanek/inteligentni-budovy-soucasnost-i-historie/>

[5] http://www.sksblansko.cz [online]. [2009] [cit. 2009-03-07]. Dostupný z:<http://www.sksblansko.cz/Article.asp?nArticleID=3&nLanguageID=1

[6] OLMER, Vít [online]. [2009] [cit. 2009-03-07]. Dostupný z: < http://hw.cz/rs-232#konvertory.

[7] KINDL, Jiří. Projektování bezpečnostních systémů I, Fakulta aplikované informatiky, Univerzita Tomáše Bati ve Zlíně, Vydání – druhé, rok 2007.

[8] TROJÁK, Pavel. *Návrh systému měření a regulace vytápění*. [s.l.], 2006. 56 s. VUT v Brně. Vedoucí bakalářské práce Ing. Stanislav Věchet, Ph.D.

[9] http://www.eurosat.cz [online]. [2009] [cit. 2009-04-15]. Dostupný z: <http://www.eurosat.cz/1979-predstaveni-systemu-concept.html>.

[10] http://www.eurosat.cz [online]. [2009] [cit. 2009-04-15]. Dostupný z: <http://www.eurosat.cz/UserFiles/Marketing/Concept/concept2006_katalog_web.pdf>.

[11] Kolektiv autorů: Názvoslovný výkladový slovník z oborů vzduchotechniky. Příloha časopisu VVI č.3, 4, 2001.

[12] Technická ochrana objektů II.díl – elektrické zabezpečovací systémy II, JUDr. Jan Uhlář, Vydavatel Policejní akademie České republiky.

[13] LACKO, Branislav. et al. Systémové pojetí automatizace. 1. vyd. Brno: Computer Press, a. s., 2000. 97 s. Všechny cesty k informacím. ISBN 80-7226-246-7.

[14] VALEŠ, Miroslav. Inteligentní dům. 2. vyd. Brno : ERA, 2008. 123 s. 21. století . ISBN 978-80-7366-137-3.

[15] TOMAN, Karel, KUNC, Josef. Systémová technika budov: elektroinstalace podle standardu EIB, 1. vyd. Praha: FCC Public, 1998. 87 s.

[16] MERZ, Hermann, HANSEMANN, Thomas, HÜBNER, Christof. Automatizované systémy budov: sdělovací systémy KNX/EIB. Václav Bartoš. 1. Auflage. Praha: Grada, 2008. 261 s. Stavitel. ISBN 978-80-247-2367-9.