České vysoké učení technické v Praze
Fakulta elektrotechnická

Bakalářská práce

Vizualizace a vzdálené řízení v síti LonWorks

Vypracoval: Martin Galbavý
Vedoucí práce: Ing. Dušan Havlík

2006

České vysoké učení technické v Praze, fakulta elektrotechnická

Katedra řídicí techniky | Školní rok: 2005/2006

Zadání bakalářské práce

Student: Martin Galbavý

Obor: Kybernetika a měření

Název tématu: Vizualizace a vzdálené řízení v síti LonWorks

Zásady pro vypracování:

1. Nastudujte principy komunikace v sítích LonWorks
2. Nastudujte současnou nabídku a možnosti prvků zabezpečovací techniky, zejména snímače otisků prstů
3. Navrhněte a nainstalujte snímač otisků prstů
4. Nastudujte způsoby a možnosti programování SW Axeda Wizcon
5. Navrhněte a implementujte vizualizaci pro ovládání budovy

Seznam odborné literatury: Dodá vedoucí práce

Vedoucí bakalářské práce: Ing. Dušan Havlík

Datum zadání bakalářské práce: zimní semestr 2005/06 (změna zadání 27. 4. 2006)

Termín odevzdání bakalářské práce: 26. 5. 2006

Prof. Ing. Michael Šebek, DrSc.
vedoucí katedry

L.S.

Prof. Ing. Zbyněk Škvor, CSc.
děkan

V Praze, dne 28. 4. 2006

Abstrakt

Práce se zabývá centrálním řízením současných automatizovaných budov. K řízení se využívá technologie LonWorks, což je jedna z možných technologií distribuované inteligence používaných k řízení automatizovaných budov. Práce je zaměřena na problematiku zabezpečení budov a především na možnosti identifikace uživatelů vstupujících do chráněných prostor a na vytvoření operátorského pracoviště řízení budovy. Navržené zabezpečení chráněných prostor a navržená vizualizace byly implementovány na fyzickém modelu administrativní budovy, který stojí na katedře Řídicí techniky ČVUT na Karlově náměstí v Praze. Vizualizace je vytvořena v prostředí Axeda Wizcon, k zabezpečení přístupu byl využit snímač otisků prstů od firmy Moeller.

Abstract

This work is about central controling of nowadays buildings. To control uses LonWorks, which is one of the possible technologies of distributed inteligence uses to control automated buildings. Thesis is directed on problems of security of buildings and above all on possibilities of identification users incoming to the protected areas and on make-up operator workplace of control building. Designed security of protected areas and designed visualization were implemented on physical model of administration building, placed at Department of Control Engineering of FEE CTU in Prague, Czech Republic. Visualization is created in environment Axeda Wizcon, to security of entry was used fingerprint sensor from firm Moeller.

Poděkování

Dovoluji si poděkovat Dušanu Havlíkovi za pomoc, kterou mi poskytl při vypracovávání bakalářské práce i za odborné konzultace. Děkuji také Pavlu Burgetovi za přátelský přístup a optimistickou podporu při realizaci. Další dík patří kolegovi Michalu Slezákovi, který mi pomohl v začátcích mé práce.

Děkuji rodině, přítelkyni a kamarádům za duševní podporu při studiu.

V Praze dne 26. května 2006 …….

podpis

Prohlášení

Prohlašuji, že jsem svou bakalářskou práci vypracoval samostatně a použil jsem pouze podklady (literaturu, projekty, SW atd.) uvedené v přiloženém seznamu.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 Zákona č.121/2000 Sb. , o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne 26. května 2006 …….

podpis

Obsah

Seznam obrázků

Seznam tabulek

1. Úvod

Termín inteligentní budova se začal používat v USA na začátku 90. let minulého století. Inteligentní budova vyjadřuje vzájemné propojení technických systémů, služeb a správy budovy, jehož cílem je splnění současných i budoucích požadavků tak, aby se maximalizovala návratnost investic. Požadavky jsou hlavně snížení provozních nákladů, ale také flexibilita budovy, kvalita vnitřního prostředí, bezpečnost a komfort.

Technické systémy budov můžeme obecně rozdělit na provozní zařízení a instalační sítě. Provozními zařízeními rozumíme např. přístupové systémy, osvětlovací zařízení, stínící prvky, sanitární vybavení objektů, HVAC[1] systémy, výtahy, kamerové systémy, protipožární okruhy a různé druhy senzorů (pohybové, senzory intenzity světla atd.). Instalačními sítěmi rozumíme rozvody, kterými do budovy přivádíme a po budově rozvádíme média a informace, např. energie, teplo, čerstvý vzduch atd.

Instalace inteligentních systémů do budov přináší mnoho výhod. Kromě snížení provozních nákladů, je to zvýšení bezpečnosti v budově, zvýšení komfortu a možnost větší flexibility při přestavování budovy. Vzhledem k těmto důvodům je instalace inteligentních systémů výhodná především v kancelářských prostorech, obchodních centrech nebo v budovách, které jsou využívány mnohostraně. Spolu s překonfigurováním např. řídicí jednotky světel můžeme využívat jiné uspořádání budovy za relativně krátkou dobu a za cenu minimálních nákladů.

Nejnovější technologie je založena na bezdrátových vysílačích (tlačítka, senzory) a přijímačích (spínací prvky) využívajících přenos frekvenčním pásmem 868 MHz, které je vyhrazeno výhradně pro použití v inteligentních budovách. Použitím RF spektra pro komunikaci mezi jednotlivými uzly odpadá nutnost montáže kabeláže a tím další snížení celkových nákladů. RF systémy se dále vyznačují především rychlou instalací a velmi vysokou flexibilitou systému.

Tato práce je rozdělena na šest částí. První část je tento úvod. V druhé části se pojednává o vlastnostech a možnostech využití sítě LonWorks a jejích základních komponent. Ve třetí části jsou nastíněny možnosti zabezpečení budov v současné době. V této kapitole jsou především popsány možnosti identifikace osob, které vstupují do zabezpečených prostor. Čtvrtá část navazuje podrobnějším popisem snímačů otisků prstů a dále pojednává o snímači Moeller M22(S)-ESA, který byl nainstalován do modelu. Pátá část popisuje existující model domovní automatizace na katedře Řídicí techniky v Praze na Karlově náměstí. Šestá část práce pojednává o komplexním programovém balíku Wizcon, ve kterém byla sestavena řídicí vizualizace pro ovládání provozních zařízení zapojených v síti LonWorks v budově.

[1] **HVAC** – Heating, Ventilating and Air Conditioning

2. Síť LonWorks

Technologii LonWorks vyvinula firma Echelon v letech 1989 až 1992 ve spolupráci s firmami Toshiba a Motorola. Na trh byla uvedena v roce 1992. Vychází z obecné definice sítě zvané Local Operating Networks (LON), tj. místní datová síť. Systém Lonworks je nejpoužívanějším systémem domovní automatizace na světě. Lonworks poskytuje otevřené řešení pro velké množství výrobců a tím vytváří konkurenční prostředí. Otevřený systém má standardizován svůj protokol, který je dostupný zájemcům, má definované standardy zařízení a funkcí a k dispozici jsou systémové softwarové nástroje. Tím je umožněno ostatním zájemcům o tuto technologii dále vyvíjet svoje vlastní zařízení a softwarové produkty. Společnost Echelon nabízí velké množství hardwarových i softwarových komponent pro stavbu sítě s distribuovanou inteligencí LonWorks. Echelon také založila organizaci LonMark, která vytváří standardy a vydává certifikáty zařízením, jež tyto standardy splňují. Komponenty, průmyslové zařízení a software založený na technologii LonWorks dnes už vyrábí a podporuje okolo 3000 firem po celém světě včetně výrobců a distributorů v ČR. Jedná se např. o osvětlovací prvky, různé druhy senzorů, digitální termostaty nebo výtahy.

Technologie LonWorks nabízí univerzální komunikaci po libovolném vedení včetně RS-485, síťového rozvodu 230V nebo rozvodu kabelové televize. Tím je vhodná nejen pro řízení spotřebičů a automatizaci budov, ale i pro dálkové odečty měřičů energií nebo regulaci v průmyslu.

Síť Lonworks je složena z inteligentních elektronických zařízení a uzlů, tzv. nódů, které mezi sebou komunikují, přijímají data ze sítě a řídí provoz na síti. Nódy vytvářejí levné a zároveň komplexně zapojené řešení automatizačního procesu. Nódy mohou být snadno integrovány i do internetové infrastruktury použitím speciálního internetového serveru založeného na LonWorks, který umožňuje přístup do sítě LON uživatelům po celém světě. Nódy jsou založeny na speciálních mikročipech nazývaných Neuron chip, na němž běží protokol LonTalk. Decentralizovaný systém využívá peer-to-peer[2] architektury s prioritním systémem zasílání zpráv. Z toho plyne výhoda nesnadného vyřazení sítě LON z provozu, neboť nemá centrální jednotku. Komunikace jednotlivých nódů je založena na sdílení informací a na vysílání zpráv při změně různých stavů a podmínek nebo jako reakci na přijatou zprávu. Každé zařízení má nadefinovány síťové proměné. Tyto síťové proměné se dělí na vstupní, výstupní a konfigurační. Virtuálním propojením dvou síťových proměných (výstupní a vstupní) lze nadefinovat komunikaci mezi dvěma zařízeními. Zařízení s výstupní proměnou odešle hodnotu této proměnné jinému zařízení nebo skupině zařízení, které si tuto hodnotu uloží do vstupní proměné.

[2] **peer-to-peer** - přímá komunikace systémem uzel-uzel

Konfigurační proměné jsou používány k nastavení parametrů komunikace jednotlivých zařízení.

Pod pojmem inteligentní rozumíme síť s distribuovanou inteligencí. Zpracovávaná veličina je distribuována mezi připojenými nódy a ty pracují nezávisle na sobě. Všechny nódy spolu komunikují jedním komunikačním protokolem – protokolem LonTalk.

Zpracovávané veličiny distribuované na síti jsou tzv. SNVT[3] proměnné. SNVT proměné jsou standardizované objekty, které mají jednoznačně určený druh přenášené veličiny včetně rozsahu a fyzikálních jednotek.

Díky univerzálnosti, otevřené formě a možnosti použití širokého spektra fyzických médií lze technologii LonWorks použít v libovolné aplikaci. Používá se zejména v obchodních centrech, výrobních továrnách, v řízení přenosu elektrické energie, v dopravních systémech od aut přes železniční dopravu až po letadla, dále se používá k řízení spotřebičů v bytech, domech až po řízení technických systémů v mrakodrapech. V komerčních aplikacích komponenty Lonworks umožňují kontrolu všech rozhodujících provozních zařízení, které jsou propojeny do jednoduchého inteligentního systému. Použití LonWorks v železniční dopravě dává strojvedoucímu a řídicímu pracovišti přehled a možnost ovlivnění funkčnosti brzdových systémů vlaku, ventilace, dveří nebo osvětlení. V domovních aplikacích lze použít speciálních inteligentních transceiverů, které využívají síťového rozvodu ke komunikaci nódů sítě LonWorks. To umožňuje zapojení spotřební elektroniky mnoha výrobců. Výrobci elektrických spotřebičů mohou použít Short Stack Developer's Kit SW od Echelonu, který umožňuje propojení sítě LON s existujícími zařízeními jako jsou např. chladnička, mikrovlnná trouba, myčka, pračka nebo sušička. V továrních halách LonWorks umožňuje zvětšení produkce a minimalizaci nákladů monitorováním a řízením manipulačních zařízení, robotů, přepravních pásů a řízení procesu výroby a její kvality. Lonworks zde umožňuje přesně načasované spouštění řízených procesů a vzdálené informování o těchto procesech. NetworkedEnergyServices od Echelonu umožňuje přeměnu rozvodné sítě na komplexně fungující rozvodnou infrastrukturu dálkově informující operátory o spotřebě energie. Zároveň zvyšuje spolehlivost dopravy energie.

Nadneseně řečeno, LonWorks umožňuje přenos dat odkudkoliv, kamkoliv a po čemkoliv. Síti LonWorks se přisuzuje dynamický rozvoj srovnatelný s internetem. Otevřený sjednocený systém založený na platformě LonWorks víceméně zásadně ovlivňuje způsob dnešního života.

Hlavní elementy a standardy využívané v síti LonWorks jsou:

- Lontalk protokol
- Neuron chipy

[3] **SNVT** – Standard Network Variable Type

- Lonworks transceivery
- Network management a aplikační software

Uvedené elementy v sobě zahrnují následující standardy:

- IFSF, CEN TC247, IEEE P1473.1 Rail Transit
- EIA 709.1 (LonTalk protokol)
- EIA 709.2 (FTT10 tranceiver)
- EIA 709.2-A-2000 (PLT22 power line transceiver)

2.1. Lontalk protokol

Protokol LonTalk byl navržen dle ISO/OSI referenčního modelu sítě firmou Echelon v roce 1989 a standardizován jako EIA 709.1. Byl navržen pro komunikaci mezi inteligentními senzory, ovládacími a akčními prvky a dalšími zařízeními v průmyslové síti. Tento typ sítí je charakteristický malými objemy přenášených dat, nízkými náklady na jednotlivé uzly, velkým množstvím různých komunikačních médií a často náročnými pracovními podmínkami (elektromagnetické rušení, prach…). LonTalk zajišťuje bezpečnou komunikaci, rychlé odezvy mezi jednotkami a poskytuje služby pro správu a diagnostiku sítě. Protokol je jako firmware částí každého uzlu v síti Lonworks.

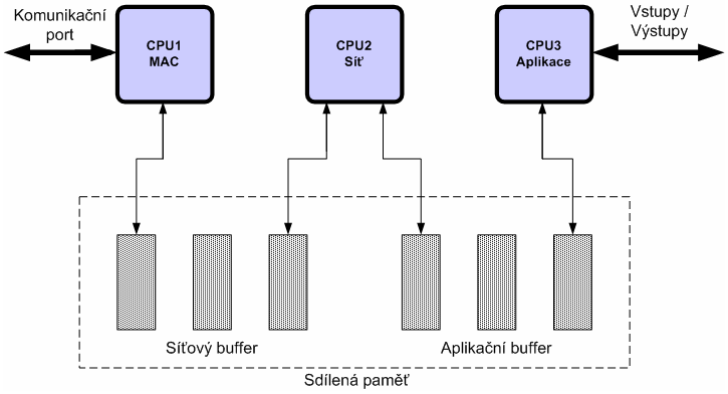
2.2. Neuron Chip

Neuron chip je hlavní komponentou technologie Lonworks. Je to mikroprocesor speciálně navržený pro rychlý a ekonomicky výhodný vývoj širokého spektra „inteligentních" akčních prvků, senzorů a i nadřazených systémů. Zajišťuje komunikaci prostřednictvím protokolu Lontalk a případně i běh uživatelské aplikace jako například komunikaci se senzory, ovládání akčních členů nebo spolupráce s jiným CPU. Skládá se ze tří osmi bitových samostatných procesorů.

CPU1 – procesor pro řízení přístupu na médium. S CPU2 komunikuje pomocí síťového bufferu. Procesor má na starosti řízení vysílání paketů dle priority, detekce kolize na sběrnici, tvorbu rámců, opravný kód CRC apod.

CPU2 – Síťový procesor. Je vyhrazený pro vytváření, příjem a zpracování síťových proměnných, autorizaci, diagnostiku provozu na síti na pozadí, časovače a čítače pro organizaci řazení paketů, vyhledávání duplicit a další. Pro komunikaci s CPU1 využívá síťový buffer, pro výměnu dat s CPU3 používá aplikační buffer.

CPU3 – Aplikační procesor. Tento procesor spouští uživatelskou aplikaci spolu s rutinami obsaženými v operačním systému Neuron Chipu. Programovacím jazykem uživatelské aplikace je Neuron C[4].



Obrázek 1 - Schéma Neuron chipu

Uživatel / programátor má možnost pomocí příkazů přímo ovládat jen aplikační CPU. Ostatní CPU již pracují samostatně a automaticky dle vnitřního firmwaru a parametrů v programu zpracovávaném v aplikačním CPU. Pro uložení aplikačního programu a aktualizovatelnývh částí firmwaru Neuron chipu se využívá jeho vnitřní Flash EEPROM paměti, případně externí paměti, což závisí na konkrétním typu Neuron chipu. Vnitřní RAM slouží pro datové proměnné aplikačního programu. Část vnitřní RAM slouží také jako prostředek pro uchování dočasných dat komunikace. Vnitřní ROM obsahuje neměnnou pevnou část firmwaru Neuron chipu. Externí softwarově ovládané I/O piny chipu mohou obvykle sloužit k libovolné komunikaci s okolím nebo pro monitorování firmwaru či čtení ID Neuron chipu.

2.3. Lonworks transceivery

Pro úspěšnou komunikaci je nutné na výstup komunikačního portu Neuron chipu připojit transceiver, který bude zajišťovat jeho ochranu, přizpůsobení a modulaci signálů pro daný typ fyzického média. Fyzickým médiem je koaxiální kabel, dvoulinka, optický kabel, radiový přenos, přenos po síťovém vedení atd.

Z hlediska napojení různých transceiverů obsahuje Neuron chip pět vývodů komunikačního portu, které lze široce softwarově konfigurovat jak po stránce funkce (klasický sériový signál proti signálové zemi, nebo pro diferenční signál apod.), tak i

[4] **Neuron C** – je klon ANSI C optimalizovaný a rozšířený pro potřeby distribuovaných aplikací v Lonworks. Používá SNVT proměnné.

po stránce nastavení komunikační rychlosti. Rychlost lze nastavovat v malých krocích od 600 bit/s do 1,25 Mbit/s a proto je možné použít různé transceivery od různých výrobců.

2.4. Network management a aplikační software

K vytváření aplikací pro síť LonWorks je potřeba vývojový software. Vývojovým softwarem pro LonWorks je NodeBuilder Development System pro PC s OS Windows dodávaný firmou Echelon. NodeBuilder Development System poskytuje vývojové prostředí a překladač pro aplikace napsané v jazyce Neuron C, Neuron C debugger, prohlížeč síťových proměných a zpráv, program Loader pro načítání nové aplikace do Neuron chipu a mnoho konfiguračních utilit pro řízení nódu. Více viz. [Echelon].

Programový balík ShortStack Developer's Kit taktéž od Echelonu umožňuje mnoha výrobcům po celém světě propojení existujících zařízení se sítí LonWorks. Tento programový balík umožňuje rychle a výrazně zvýšit funkčnost inteligentních zařízení a spotřební elektroniky, které jsou založené na osmi, šestnácti nebo třicetidvou-bitových mikročipech. Tato zařízení pak mohou komunikovat mezi sebou přímo po síti LonWorks nebo s využitím internetu. Plná verze ShortStack Developer's Kit je ke zdarma ke stažení na stránkách Echelonu, viz. [ShortStack].

3. Zabezpečovací technika

Jedním z požadavků moderní budovy je dostatek bezpečí. Se vzrůstajícím počtem krádeží vloupáním a se současným snižováním cen zabezpečovací techniky je stále více bytů či domů vybaveno zabezpečovacím systémem. V dnešní době jsou systémy ochrany majetku a osob nepostradatelnou součástí vybavení moderních prostor. Instalace inteligentních prvků do zabezpečovacích okruhů přináší kromě výhody snížení ceny řešení též možnost širokého spektra programování systému. Při narušení systému hlavními vchodovými dveřmi lze např. nastavit prodlevu aktivace poplachové sirény, potřebnou k deaktivaci poplachu zadáním uživatelského hesla na klávesnici vyhodnocovací jednotky. Při narušení jakékoli jiné zóny dříve než vstupních dveří se siréna může spustit hned, a systém může sám přivolat policii nebo bezpečnostní agenturu. Majitel může být informován o narušení svého objektu GSM modulem. Do programu systému může být zavedeno několik stupňů zabezpečení, např. odjezd majitele na delší dobu tzv. noční hlídání, které se vyznačuje přítomností majitele uvnitř objektu.

Nezbytným předpokladem kvalitního elektronického zabezpečovacího systému je dostatečně silný náhradní zdroj energie. Současné systémy se vyvíjí

směrem ke komplexním systémům, které využívají několika stupňů ochrany a v případě vstupních systémů několika stupňů autentizace. Obecně je v těchto systémech velice důležité využívat několika aktivních záloh, ať už se jedná o náhradní zdroj energie nebo přenosovou cestu na pult centrální ochrany, aby v případě výpadku proudu nebo odstranění přenosové cesty útočníkem zbývalo ještě záložní řešení.

Možnosti zabezpečení objektu se rozdělují na několik kategorií:

- Elektronické zabezpečovací systémy (EZS),
- Perimetrické (obvodové - venkovní) zabezpečovací systémy (PER),
- Napojování na pulty centralizované ochrany (PCO),
- Mechanické zábranné systémy (MZS),
- Vstupní systémy
    - Docházkové systémy,
    - Systémy kontroly přístupu do zabezpečených zón,

Elektronický zabezpečovací systém EZS je soubor zařízení složený z několika částí tvořících komlexní zabezpečovací řetězec. Mezi zařízení tvořících EZS patří senzory (pohybu…), kontaktní senzory, ústředny, sirény, přenosové prostředky a signalizační nebo ovládací pulty. EZS monitoruje vstup neoprávněných osob do střežených prostor a následně při narušení objektu vyhlašuje poplach a dává pokyn k přivolání policie, bezpečnostní služby nebo informuje přímo majitele objektu pomocí GSM modulu. Tyto systémy spadají pod státní normu ČSN EN 50131, která zavádí termín poplachové systémy, určuje minimální požadavky a parametry zařízení, a definuje osoby, které mohou instalaci provádět.

Perimetrická ochrana (PER) je venkovní obvodová ochrana areálu. Je to soubor technických, elektronických, popřípadě elektro-mechanických aplikací venkovních zabezpečovacích systémů. Je nezbytnou součástí rozlehlých prostorů, které mají zvýšený stupeň zabezpečení. Příkladem jsou komerční budovy, obchodní centra, stadiony, vývojové laboratoře, věznice, letiště apod. Hlavním úkolem perimetrické ochrany je zachytit případného narušitele předtím než se dostane do střeženého prostoru. V kombinaci s kamerovým systémem a rozeznáváním osob na dálku se jedná o velmi účinný systém ochrany majetku.

Napojením na pulty centralizované ochrany (PCO) přebírají úlohu vyhlašování poplachu od sirén přenosová zařízení, která po zvoleném médiu (RF, GSM modul, telefonní linka, satelit…) zprostředkovávají informaci o narušení objektu majiteli, bezpečností agentuře nebo ji posílají na monitorovací pracoviště

PCO policie. Používané formáty přenosových paketů spadají pod normu ČSN EN 50136. Na rozdíl od vyhlášení poplachů v místě narušení přináší připojení elektronických systémů na pulty centrální ochrany výrazně efektivnější ochranu objektu. Elektronickými systémy rozumíme elektronické zabezpečovací systémy, elektronické protipožární systémy a systémy průmyslových kamer.

Mezi mechanickými zábranné prostředky (MZS) patří zejména prostředky pro ohraničení prostor, např. zdi a ploty, vstupní mechanické bezpečnostní systémy vrat, dveří a oken, mříže, bezpečnostní skla a fólie a uzamykací systémy. Do této skupiny patří také prostředky pro uschování majetku – trezory. Základní úlohou mechanických zábranných systémů je vytvořit pevnou překážku proti násilnému vniknutí osob a zabránit znehodnocení a krádeži předmětů, techniky a zařízení umístěných v chráněném objektu.

Docházkové systémy (DS) slouží ke sběru informací o čase a důvodu průchodu nebo průjezdu místem kontroly a jejich dalšímu zpracování s vazbou na zpracování docházky a možností úplné náhrady tzv. „píchacích hodin“ na pracovišti v kombinaci s některou metodou rozpoznání (verifikace) uživatele. Tyto systémy se také využívají např. v garážových prostorech.

Systémy kontroly a řízení vstupu v bezpečnostních aplikacích (ACS / Acces Control Systems) hlídají vstup do chráněných prostor a vstup do těchto prostor umožňují pouze uživateli, který se prokazuje nějakou metodou autentizace. Mezi používané metody patří autentizace heslem, autentizace předmětem (kartou…) a biometrická autentizace (viz. dále). ACS systémy spadají pod normu ČSN EN 50133.

Verifikace značí ověřovací proces v systému ACS, který vždy vyžaduje přihlášení uživatele do systému, kde je poté provedeno porovnání naskenovaného záznamu se záznamem v databázi. Je důležité omezit počet možných přihlašovacích pokusů než bude uživatel systémem definitivně odmítnut jako nepovolaná osoba. Pro daný počet přihlašovacích pokusů je nutné vzít v úvahu úroveň zabezpečení systému. Čím menší počet pokusů zvolíme tím s větší pravděpodobností vyvoláme několik falešných poplachů kvůli neprovedené identifikaci oprávněného uživatele. Na druhou stranu je ale nutné zvolit takový počet pokusů, aby neoprávněný uživatel neměl čas získat dostatek informací o systému, které by mu později pomohly systém prolomit.

U vysoce zabezpečených systémů by měly být výsledky verifikace pro pozdější zpracování ukládány. Nabízí se dvě možnosti a to konkrétně přímo do snímače (do hlavní jednotky snímače) a nebo do vzdáleného počítače. Ukládání přímo do snímače je nevýhodné vzhledem k omezené paměti jednotky. Při plné

paměti by starší záznamy byli pravděpodobně přemazávány novějšími. Při ukládání do vzdáleného počítače není proces omezen velikostí paměti, ale existuje určité nebezpečí průniku do systému zvnějšku, čili je nutné tuto komunikaci dále zabezpečit.

Pro ukládání do centrální databáze znaků (identit) existuje několik možností. Centrální databáze je databáze, ve které jsou uložené všechny vzory identit pro porovnávání, např. uložená přístupová hesla nebo vzory pro biometrickou identifikaci. Lze ukládat přímo do snímací jednotky, ukládat do vzdáleného počítače a nebo ukládat znaky do tokenu. Každá možnost má své pro a proti. Ukládání znaků přímo do jednotky je nevýhodné, podobně jako u ukládání verifikačních dat, vzhledem k omezené paměti. Proto je tento způsob používán u systémů s ne mnoha uživateli. Druhý způsob, ukládání do vzdáleného počítače s sebou přináší problémy se zabezpečením jak už počítače, ve kterém databáze je, tak hlavně komunikační cesty. Třetí způsob, ukládání dat do tokenu, je nevýhodné z hlediska nutnosti složitější elektroniky a rozhraní pro token, tedy z hlediska ceny řešení a stupně zabezpečení.

Každý systém automatizovaného přístupu je závislý na kvalitě mechanismu, kterým je zabezpečen přístup. Existují tři hlavní principy autentizace:

Autentizační mechanismy		
Mechanismus	**Příklad**	**Terminologie**
co uživatel zná	heslo	Autentizace heslem
co uživatel má	autentizační předmět	Autentizace předmětem
co uživatele charakterizuje	otisk prstu	Biometrická autentizace

Tabulka 1 - Přehled autentizačních mechanismů

Kvalita autentizační metody je dána poměrem mezi počtem možných pokusů a jednoznačností rozlišení dané metriky. Pro popis se používají následující tři koeficienty:

- Koeficient chybného přijetí (*False acceptance* „FAR“)
  vyjadřuje pravděpodobnost s jakou systém vyhodnotí neoprávněnou osobu jako oprávněnou,
- Koeficient chybného odmítnutí (*False rejection* „FRR“)
  vyjadřuje pravděpodobnost s jakou systém vyhodnotí oprávněnou osobu jako neoprávněnou,
- Koeficient vyrovnané chyby (tzv. křížový koeficient)
  koeficient, který se nalézá ve středu mezi FAR a FRR, kde tyto situace mohou nastat se stejnou pravděpodobností.

3.1 Autentizace heslem

Autentizace heslem patří stále k nejpoužívanějším typům autentizace. Princip zabezpečení spočívá v tom, že si uživatel zapamatuje několika místné heslo, které zadává při přístupu do chráněné oblasti. Heslo obsahuje nejčastěji číslice, méně častěji už znaky. Tyto typy hesel jsou v současné době nejvíce používány k zabezpečení telefonních SIM karet nebo platebních karet (PIN heslo), e-mailových účtů, kont v počítačích,.

Výhody zabezpečení heslem jsou zejména lehká realizovatelnost a cena zabezpečení. Nevýhod je celá řada která omezuje aplikace na systémy s minimálními bezpečnostními požadavky. Mezi největší nevýhody patří nízká bezpečnost, možnost dekódování dekódovacím programem, možnost zapomenutí, zneužití cizí osobou apod.

Dobře zvolené heslo obsahuje malá i velká písmena i další znaky dostupné na klávesnici. Heslo má dostatečnou délku a je distribuováno zabezpečeným způsobem. Mělo by být pouze zapamatováno a nikde nepoznamenáno. Nemělo by jít též o obvyklé slovo nebo známou frázi a nemělo by ho být možné odvodit ze znalosti osoby vlastníka hesla. Také by mělo být jednou za čas obměňováno.

3.2 Autentizace předmětem

Autentizace předmětem se opírá o vlastnictví předmětu, který je pro autentifikaci vyžadován. Tento předmět se nazývá *token*. Token je jedinečný a nekopírovatelný, respektive těžce kopírovatelný. Tokeny jsou vybaveny informací, která je používána při provádění autentizačního protokolu. Tím se ověřuje identita uživatele. Výhodou tokenu která je zároveň jeho nevýhodou, je jeho přenosnost. Proto by měly systémy, které vyžadují větší bezpečnost používat token v kombinaci s heslem.

Používanými autentizačními předměty jsou:

- **Tokeny pouze s pamětí** (magnetické, elektronické nebo optické karty) – jsou obdobou mechanických klíčů,
- **Tokeny udržující hesla** – vyžadují zadání uživatelského hesla, např. platební karty s PINem
- **Tokeny s logikou** – umějí zpracovávat jednoduché podněty typu vydej: následující klíč, vydej cyklickou sekvenci klíčů,
- **Inteligentní tokeny** (smart cards) – mohou mít vlastní vstupní zařízení pro komunikaci s uživatelem, vlastní časovou základnu a mohou šifrovat nebo generovat náhodná čísla apod.

3.3. Biometrická autentizace

Biometrika není sice novým oborem avšak v poslední době dochází k jejímu prudkému rozvoji. Název je odvozen ze dvou řeckých slov „bios“ a „metric“, čili měření živých organismů. Biometrika využívá jedinečných tělesných znaků pro identifikaci osoby. Výhodou tohoto typu autentizace je, že není nutné pamatovat si několika místné kombinace hesel či neustále s sebou nosit snadno zcizitelný token, např. přihlašovací kartu. Biometrická autentizace je rychlou a pohodlnou a velice přesnou metodou, která je navíc levným řešením, vzhledem ke svým neexistujícím pozdějším nákladům. Její hlavní výhodou je skutečnost, že biometrické charakteristické znaky zůstávají během života neměnné a nelze je ukrást či zapomenout.

Podstatou všech biometrických systémů je automatizované snímání biometrických charakteristik a jejich následné porovnávání s údaji předem sejmutými do centrální databáze charakteristických znaků. Zabezpečení centrální databáze má vliv na celkovou bezpečnost systému. Hacker, který by se dostal k citlivým údajům, by je totiž mohl snadno zneužít.

Současné biometrické systémy pracují s různými charakteristickými znaky člověka. Používanými metodami jsou technologie snímající otisky prstů, metody rozpoznávání obličeje v davu osob, snímání struktury oka, metody snímání fyziologického tvaru ruky a zkoumání spektra hlasu. Cílem v oblasti bezpečnosti je vytvoření komplexních systémů založených na kombinaci měření více charakteristik. Tím se bezpečnost těchto systémů mnohonásobně zvýší. Následuje popis nejpoužívanějších biometrických systémů:

3.3.1. Verifikace otisku prstu

Verifikace otisku prstu se opírá o fakt, že otisk prstu je jedinečný a zůstává neměněn po celý život. Verifikace otisku prstu je nejčastější používanou biometrickou metodou. Senzor otisku prstu snímá a vyhodnocuje přiložené otisky. Podle způsobu snímání rozeznáváme několik různých typů senzorů. Z naskenovaného otisku je vytvořena jeho předloha podle relativního umístění charakteristických rýh a prohlubní. Tato předloha je poté porovnávána se vzorem uloženým v databázi.

Senzory otisků prstů se používají u různě vysokých stupňů zabezpečení. Jejich nevýhodou je, že u nich poměrně často nastává jev chybného odmítnutí podle typu snímací metody a úrovně zašpinění otisku prstu.

3.3.2. Verifikace tvaru ruky

Metoda verifikace tvaru ruky je založena na měření fyzikálních charakteristik ruky a prstů. Hlavními zkoumanými parametry je délka a šířka dlaně a jednotlivých prstů, boční profil ruky apod. Používá se speciální snímač, který vytváří 3D obrázky a získaná data ukládá do devíti bytové hodnoty. Tímto je metoda velmi vhodná v aplikacích, kde je omezená paměť pro ukládání těchto dat. Z tohoto důvodu a z hlediska snadného používání je také velmi vhodná do aplikací, kde je více uživatelů.

3.3.3. Verifikace obličeje

Verifikace obličeje je dnes nejvíce zkoumanou biometrickou metodou. Veškerá technologie vychází z faktu, že lidský obličej obsahuje kolem 80 typických rysů. K úspěšné identifikaci osoby stačí rozpoznání 14 až 20 z nich. Metoda rozpoznání obličeje vychází ze srovnání obrazu z kamery s obrazem uloženým v databázi. K jednoznačné identifikaci slouží tvar obličeje a poloha rtů, nosu, očí nebo obočí. V centrální databázi je uložena relativní poloha, tedy vzdálenost očí, úhel od špičky nosu k oku apod.

Tento druh verifikace nachází uplatnění např. u docházkových systémů zaměstnanců, kde by mohl zcela nahradit stávající tzv. „píchačky“.

3.3.4. Verifikace hlasu

Metoda rozpoznávání hlasu osoby vychází z rozšířené analýzy hlasu zaznamenaného mikrofonem. Předpokladem jednoznačnosti je, že žádná osoba nemá stejný tvar hlasivek, ústní dutiny, jazyka nebo zubů a tudíž ve výsledku má jedinečný hlas. K nejúspěšněším technikám ověřování hlasu patří porovnávání vzorků řeči z hlediska jeho spektra. Nevýhodou této metody může být složitější vyfiltrování užitečného signálu z pozadí ruchu okolí. Dalším problémem může být nastydnutí uživatele, kdy se z důvodu nachlazených dýchacích orgánů nebo nosu změní hlas. Naopak výhodou metody je její snadné používání, rychlost a spolehlivost.

3.3.5. Verifikace sítnice

Pro ověření osoby pomocí její sítnice se používá digitální obraz struktury sítnice v okolí slepé skvrny oka. Sítnice je světlo-citlivý povrch na zadní straně oka. Je složena z velkého množství nervových buněk převádějících světlo na nervové signály. Slepá skvrna na zadní straně oka je místo kde z něj vystupují nervová

vlákna. Pro získání digitálního obrazu se používá zdroj světla s nízkou intenzitou záření a optoelektronický systém. Cíl skenování se nachází v okolí slepé skvrny oka. Naskenovaný obraz je převeden do podoby čtyřiceti bytového čísla.

Verifikace sítnice je velice přesnou metodou identifikace. Její používání vyžaduje od uživatele, aby se díval do přesně vymezeného prostoru, což může být pro některé osoby nepříjemné a někdy až nemožné, pokud používají brýle. Z těchto důvodů nemá tato metoda rozšířenou oblast používání a její použití se shrnuje na oblasti vůbec nejvyššího stupně zabezpečení.

3.3.6. Verifikace duhovky

Verifikace duhovky je druhá metoda, která využívá jedinečnosti oka. Duhovka obsahuje tolik jedinečných charakteristických znaků, že je mnohonásobně přesnější metodou než např. verifikace otisku prstu. Duhovky dvojčat jsou různé a dokonce duhovky jednoho člověka jsou také odlišné. Proto je tato metoda velice přesnou metodou identifikace.

4. Snímače otisků prstů

Snímače otisků prstů patří do skupiny biometrických snímačů. Otisk prstů je unikátní identifikační znak každého člověka. Zůstává nezměněn od zhruba půl roku života. Nemůžeme ho přenášet, zapomenout ani ztratit. Různé osoby nemohou mít stejné otisky. Stejný otisk prstu nemají ani jednovaječná dvojčata.

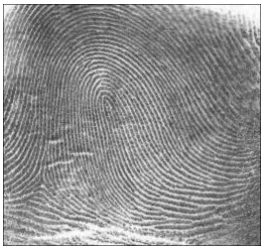
V poslední době se snímače otisků prstů používají stále častěji k zabezpečení nejen vstupů do budov, ale i jako identifikace oprávněného uživatele PC (např. notebooku) nebo flash disku. Rozsah použití je velmi široký.

Otisky prstů jsou jedni z biometrických klíčů používaných k unikátní identifikaci člověka a ověřování jeho identity. Analýza otisků prstů sestává z hledání *minutiea*. Minutiea jsou rýhy a prohlubně, čili detaily papilárních linií. Zkoumá se jejich vzájemná relativní poloha. Na rozdíl od přímého porovnávání například naskenovaných obrázků otisků je toto klíčem k rychlému porovnání sejmutého otisku a toho uloženého v databázi.

Typy papilárních linií		
Název	**anglický výraz**	**pravděpodobnost výskytu**
smyčky	loop	60 až 70 %
víry	shodl	25 až 35 %
oblouky	arch	cca 5 %

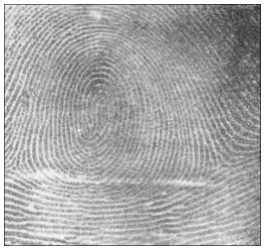
Tabulka 2 - Typy papilárních linií

Papilární linie (angl. pattern) je souhrn charakteristických znaků minuteí. Jsou to tzv. klasifikační vzory a rozdělují se do tří základních skupin, jsou to smyčky, víry a oblouky (viz. následující obrázky). Rodinní příslušníci často zdědí tyto vzory po svých předcích.



Obrázek 2a - Smyčka

Obrázek 2b - Oblouk



Obrázek 2c - Vír

Hlavní rysy minutiea jsou ostrůvky, mosty, ukončení linie, rozdvojení, roztrojení a překřížení. Minutiea a typy papilárních linií jsou nejdůležité faktory při analýze otisků prstů.

Obrázek 3 - Některé minutiea - zleva ostrov, most, rozdvojení, roztrojení, překřížení

Senzor otisku prstu je elektronický přístroj, který snímá a vyhodnocuje digitální obraz přiloženého otisku prstu. Sejmutý obraz je nazýván live-scan, který je digitálně zpracován a je z něj vytvořen vzor (template[5]). Vzor je uložen v databázi spolu s ostatními k pozdějšímu porovnávání.

Není možné zaručit naprostou funkčnost systémů díky některým otiskům prstů a jejich následným zpracováním vnitřní elektronikou. Problémy s použitím se můžou stát především díky zranění, příliš hladkým otiskům nebo hlavně díky tlustým liniím. V některých situacích, závisejících na parametrech algoritmu, vnitřní elektronika může vyhodnotit otisk tak, že je buď chybně odmítnut (false rejection, FRR), nebo ve velmi málo případech naopak chybně přijat (false acceptance, FAR). Nejčastějšími důvody které v některých případech vedou ke špatné identifikaci jsou například zranění, suchá kůže, špína, vlhkost, špatně vložený prst, prsty s málo zhodnocenými rysy nebo velmi podobné otisky mohou v některých případech vést ke špatné identifikaci.

[5] **Template** je soubor popsaných charakteristických znaků

4.1. Typy senzorů

Protože existuje několik metod snímání otisku prstu, senzorů je také několik druhů. Liší se mezi sebou kromě metody snímání také různými parametry, např. náchylností k zašpinění. Důsledkem zašpiněného prstu může být chybné odmítnutí, což je zejména u optických a tepelných senzorů častým jevem.

4.1.1. Optické senzory

Optické senzory patří mezi nejstarší technologie snímání otisku prstu. Hlavní princip spočívá v přidržení prstu nad skleněnou podsvětlenou vrstvou. Optický senzor zachycuje digitální obraz otisku použitím viditelného světla. Světlo se odráží z prstu a prochází přes tuto vrstvu do CCD snímače, který zachycuje vizuální obraz otisku. Nevýhoda tohoto typu je, že je poměrně náchylný k chybám. Například pouhý špinavý prst vede ke špatnému obrazu. Z toho vyplývá nutnost opakovaného skenování prstu a vyšší nároky na údržbu, protože nečistoty z rukou zůstávají na skenovací plošce.

4.1.2. Ultrazvukové sensory

Ultrazvukové senzory narozdíl od optických, které měří odražené světlo, měří odraženou zvukovou vlnu. Technologie funguje na podobných principech jako sonar. Jejich výhodou je, že ultrazvuk snadno pronikne i nečistotami, které by znehodnotili obraz zachycený pomocí optického snímače.

4.1.3. Kapacitní senzory

Kapacitní metoda snímání měří velikost elektrického pole mezi rýhami a prohlubněmi v papilárních liniích prstu. Měření se provádí pomocí několika desítek tisíc kondenzátorů, které jsou sestaveny do organizované sítě. Pomocí této sítě je sestaven obraz otisku. Kapacitní senzory patří k přesnějším systémům identifikace otisku prstů.

4.1.4. Teplotní senzory

U teplotního senzoru teplotní senzor snímající otisk prstu měří teplotní rozdíly mezi jednotlivými rýhami na prstu a vytváří z nich digitální obraz prstu. U tohoto druhu senzoru, na rozdíl od jiných, je nutné přejet prstem po ploše senzoru. Obraz je snímán postupně po obdélnících velikých jako je plocha senzoru. Poté je výsledný obraz složen pomocí různých metod zpracování obrazů. Vzhledem k tomu,

že senzor snímá teplo je schopný rozpoznat pravý otisk od neživé napodobeniny. Nevýhodou je stejně jako u optických senzorů nutnost častěji čistit skenovaní plošku.

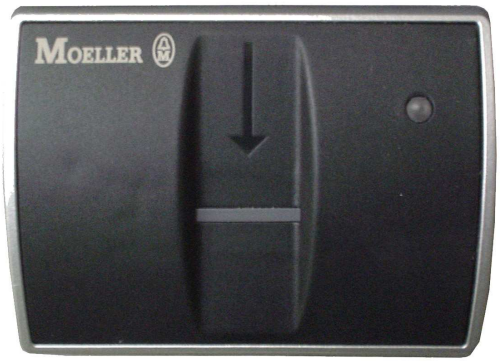
4.2 Snímač otisků prstů Moeller M22(S)-ESA

Pro zabezpečení vchodových dveří kanceláře č.1 modelu administrativní budovy byl vybrán snímač otisků prstů Moeller M22(S)-ESA. Tento senzor s integrovaným spínačem a digitálním zobrazovacím panelem byl připojen na krokový motorek. Tento motorek je mechanicky připojen na systém otevírání dveří. Po kladné identifikaci uživatele je sepnuto spínací relé na výstupu snímače a následuje otevření vchodových dveří. Na zobrazovací jednotce je zobrazeno jméno uživatele.

4.2.1. Popis snímače

Biometrický klíč Moeller M22-ESA je průmyslový spínač s integrovanou technikou pro snímaní otisků prstů. Je založen na tepelné metodě snímání. V prvním kroku se musí přejet prstem ruky přes senzorovou jednotku, vyznačenou na obrázku 4b. Naskenovaný obraz je porovnán s otiskem uloženým v paměti přístroje a přístup do místnosti je buď povolen nebo zakázán. Respektive je sepnuto relátko na výstupu snímače, které je použito k ovládání servomotorku vstupních dveří. Status přístroje je zobrazován pomocí integrovaných LED. Zelená barva značí připravenost přístroje na identifikaci, oranžová značí že je přístroj zaneprázdněný a červená barva značí chybu. Napodobení otisku je obtížnější díky měření teploty, neboť tím lze identifikovat živou tkáň od neorganické napodobeniny.

Obrázek 4a - Operační jednotka MFD-80-(B)



Obrázek 4b - Senzorová jednotka M22(S)-ESA1

Ukládání nových uživatelů do databáze přístroje má tři kroky. Přiložený otisk prstu je nejprve třikrát sejmut, jsou vyhodnoceny všechny podobnosti a odchylky, které jsou způsobeny např. ne vždy stejně silným přiložením prstu, nestejnou vlhkostí a i nestejným směrem nebo rychlostí přiložením prstu. Digitální obraz otisku je poté uložen do paměti. Do paměti lze uložit maximálně 100 otisků prstů, které můžou být rozděleny do tří různých uživatelských skupin dle stupně autorizace. Stupeň autorizace se určuje dobou sepnutí výstupního relé.

Přístup do paměti nastavení parametrů přístroje je zabezpečen 6-místním číselným kódem. Tento kód je nastaven z výroby na *000000*. Pokud je kód nastaven na tuto kombinaci, je zároveň deaktivován a není vyžadováno jeho zadání při změně parametrů přístroje. Pokud je kód změněn, je zároveň aktivován a bez jeho znalosti není zpřístupněna možnost měnit nastavení přístroje, editovat uživatele nebo vkládat nové uživatele.

Kompletní jednotka M22(S)-ESA se skládá ze čtyř částí:

- M22(S)-ESA1 –přední část jednotky, obsahuje senzor potřebný pro snímání
- M22-ESA-R – zadní část M22-ESA-R, obsahuje vyhodnocovací elektroniku
- MFD-80-B – display
- MFD-CP4 – operační jednotka, na jejíž přední stranu se připojuje MFD-80-(B)

4.2.2. Popis identifikace

Identifikace je založena na nejnovějších algoritmech zpracování obrazů, které mají potřebnou rychlost pro práci v reálném čase.

Systém přečte otisk prstu přejetím prstu přes senzor. Software předzpracování obrazu optimalizuje obrázek tak, že ve výsledku jsou uloženy pouze linie otisku. Rušivé signály jsou eliminovány. Poté jsou rozpoznány charakteristické rysy. Jako Vzor (template) je uložen typ rysů (rozvětvení, víření, ostrovy, elipsy atd.) a jejich vzájemná relativní poloha. Vzor je soubor dat, ve kterém je otisk prstu popsán podle jeho rysů. Jeho výhodou je velikost uložených dat. V porovnání s obrázkem je mnohem menší.

Obrázek 5 – Znázornění postupu vytvoření template otisku

Vzor právě čteného otisku je poté porovnáván s již uloženými vzory. Pokud odpovídá dostatečné množství shodných rysů, je otisk identifikován jako platný a sepne se relátko na výstupu snímače. Pokud neodpovídá dostatek rysů je otisk odmítnut.

4.2.3. Zapojení systému

Nejprve je nutné vybalit všechny části z krabice. Jedná se o senzorovou jednotku M22-ESA1, základní jednotku M22-ESA-R a operační jednotku MFD-CP4 s displayem MFD-80-(B). Dále si připravíme kabely pro napájecí napětí 24V, propojovací kabel MFD-CP4-800 který je komunikačním rozhraním mezi snímací jednotkou a zobrazovací jednotkou MFD-CP4+MFD-80-(B). Postup zapojení systému je uveden na následujících řádcích.

1. Senzorovou jednotku M22(S)-ESA1 připojit na základní jednotku M22-ESA-R
2. Display MFD-80-(B) připojit na jeho operační jednotku MFD-CP4
3. Na dvoupólový terminál připojit napájecí napětí +24V DC a zem 0 V DC.
4. Výstupní relé snímací jednotky připojit na ovládací motorek dveří. (Nesmí být překročen maximální spínací proud 3A nebo 15 – 230 V AC)
5. Zařízení připojit pomocí kabelu MFD-CP4-800 k operační jednotce MFD-CP4. (Zařízení může být připojeno též k PC pomocí kabelu EASY800-PC-CAB. tato část se může provést až po 3. bodě nastavení systému)

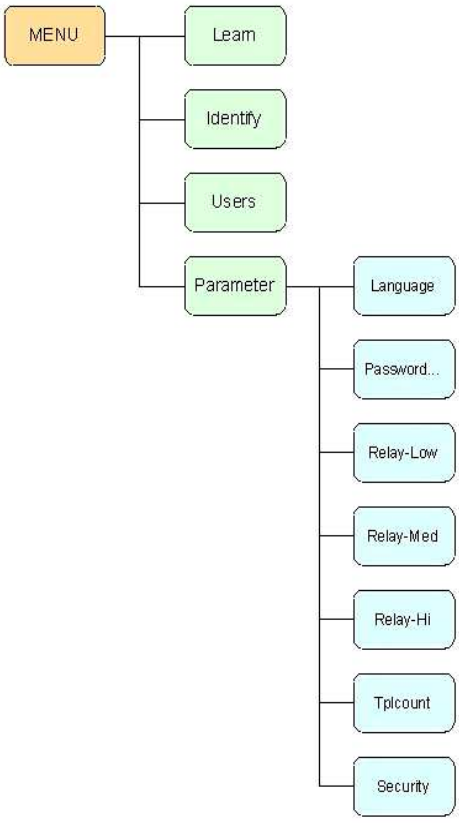
Barva LED	Popis
Zelená	Systém čeká na identifikaci
Oranžová	Identifikovaný otisk je kontrolovaný. Během této operace není možná další identifikace
Červená	Otisk neodpovídá žádnému vzoru v paměti
Červená blikající	Chyba, otisk nebylo možné zkontrolovat

Tabulka 3 - Popis stavů LED na snímací jednotce M22(S)-ESA1

4.2.4. Nastavení systému

Po vzájemném propojení všech komponent a po připojení k napájecímu napětí je systém připraven k použití. Po prvním zapnutí je uživatel dotázán na jazyk, ve kterém bude systém komunikovat. Postup je vyznačen v následujících bodech.

1. Zapnout napájecí napětí
2. Po zapnutí napájení zařízení provede kontrolu funkčnosti sám sebe (self-check). LED svítí nejprve krátce červeně, pak oranžově bliká a pak svítí zeleně.
3. Zvolit jazyk ve kterém chceme aby zařízení komunikovalo (anglicky nebo německy). Nejprve je nutné stisknout tlačítko *OK*, poté pomocí kurzorových šipek vybrat požadovaný jazyk. Potvrzení se provádí stisknutím tlačítka *Esc*.



4.2.5. Popis Menu

Standardní nabídka přístroje se skládá z následujících podnabídek:

- **Learn**
  (načítání nových uživatelů do paměti)
- **Identify**
  (systém vyčkává na identifikaci otisku)
- **Users** (seznam uložených uživatelů)
- **Parameter** (nastavení parametrů systému)
- **Diagnosis**
  (tato nabídka je pouze pro servisní účely. Zařízení si provede Self-Check)

Obrázek 6 - Hlavní body nabídky zařízení MFD-Titan

4.2.5.1. Menu Learn

Toto menu je klíčovou nabídkou pro pozdější chod snímače. Zde je možnost zadat do paměti až 100 otisků prstů. Na kvalitě sejmutých otisků prstů respektive na kvalitě vzoru vytvořeného ze sejmutých otisků je značně rozhodující kvalita pozdější

identifikace. Pokud je kvalita nízká, proces identifikace provází vyšší četnost jevu chybného odmítnutí FRR. Z sejmutého otisku zařízení vytvoří nejprve počet vzorů které máme nastaveny v menu *parameter - tplcount*, a později je uloží společně do jednoho vzoru. Tento proces je nazýván *merge*. Po tomto procesu obsahuje vzor vysoký počet charakteristických rysů otisku. Sejmutý otisk je uložen pod názvem *USERxxx* do centrální databáze otisků, kde xxx značí pořadové číslo uživatele.

Pokud má systém načteno více rysů otisku, pracuje lépe. Následuje krátký seznam doporučených pravidel, jak používat systém tak, abychom maximalizovali schopnosti rozeznávání senzoru:

- Prstem přejet přes snímač konstantní rychlostí (0,5 – 1 s) v jedné linii směrem od shora dolů.
- Prstem přejet přes snímač tak, aby mohl načíst co nejširší, největší a co nejrovnější plochu otisku.
- Vždy přes snímač přejet tak, jak má zaznamenáno v paměti (ve stejném směru, stejným prstem atd.)
- Přes snímač přejet tak, aby mohl přečíst co nejvíce charakteristických rysů otisku
- Snímač udržovat v čistotě a občas otřít skenovaní plošku, na které ulpívají nečistoty z prstů.

Obrázek 7 - Menu Learn

4.2.5.2. Menu Identify

V tomto stavu čeká zařízení na příchozí otisk prstu. Dioda na zobrazovací jednotce MFD-Titan a na snímacím modulu M22(S)-ESA1 svítí zeleně. Po přejetí prstem po skenovaní plošce je z tohoto live-scanu vytvořen vzor, který je dle umístění charakteristických bodů porovnáván se vzory uloženými v databázi. Pokud je příchozí otisk stejný s tím, který je v databázi, je identifikace vyhodnocena kladně

a sepne se relé na výstupu jednotky. V případě, že v databázi není uložen žádný otisk, objeví se chybová hláška *No users*.

4.2.5.3. Menu Users

V této nabídce je centrální databáze sejmutých otisků prstů – jejich vzorů. Max. velikost této databáze je 100 otisků. V databázi jsou uložené všechny otisky, které byly identifikovány v menu *Learn*. Každému otisku pojmenovanému *USERxxx* lze v této nabídce přiřadit jméno a stupeň autorizace. Velikost jména je max. 8 znaků.

- Ovládání je kurzorovými klávesami a tlačítkem *OK*. Kurzorovými klávesami měníme postupně znaky abecedy.
- Tlačítko *Alt* nastavuje autorizaci.

4.2.5.4. Menu Parameter

V této nabídce je veškeré uživatelské nastavení snímače. Zde je možnost nastavení možné relativní míry „FAR“ nebo „FRR“, což jsou parametry které ovlivňují především počet možných chybných identifikací. Parametry zařízení jsou rozděleny do dvou skupin:

1. Systémové parametry
   - Jazyk
   - Heslo
   - Spínací časy relé dle nastavené autorizační úrovně

2. Parametry pro identifikaci otisku
   - Tři hodnoty bezpečnostní úrovně (nízká bezpečnost, střední a vysoká)
   - Počet vzorů které se použijí v režimu učení.

Pro ovládání se používají tyto klávesy:

- ↑↓ - kurzorové šipky pro pohyb,
- *ESC* nebo → - návrat do hlavního menu,
- *OK* nebo ← - potvrdí změnu hodnoty,
- *ALT* - nastaví parametr na jeho standardní hodnotu.

Stisknutím tlačítka *OK* lze parametr editovat.

Následující tabulka ukazuje možnosti editace parametrů přístroje:

Menu Parameter		
Language (jazyk)	English Deutsch	Výběr jazyka – anglicky, německy. Default: anglicky
Password... (heslo...)	Change Password Admin Logout	Nastavení hesla. Default: 000000 (pokud zadáme jako heslo 000000 znamena zaroven deaktivování hesla). Pokud je nastaveno heslo, položka „Admin logout“ heslo aktivuje.
Relay-Low	1 - 10s	Spínací čas relé. Pro uživatele s nejnižší autorizací (v sekundách). Default: 1 sekunda
Relay-Med	1 – 10s	Spínací čas relé. Pro uživatele s normální autorizací (v sekundách). Default: 2 sekundy
Relay-Hi	1 – 10s	Spínací čas relé. Pro uživatele s nejvyšší autorizací (v sekundách). Default: 3 sekundy
Tplcount	1 – 5	Kolik použije zařízení vzorů pokud se „učí“ otisk nového uživatele. Default: 3 vzory
Security (bezpečnost)	„Low“ (nízká) „Med“ (střední) „Hi“ (vysoká)	„Low“ – nízký FRR a s ne-častými FAR „Med“ – střední FRR s několika FAR „Hi“ – vysoké FRR s častými FAR

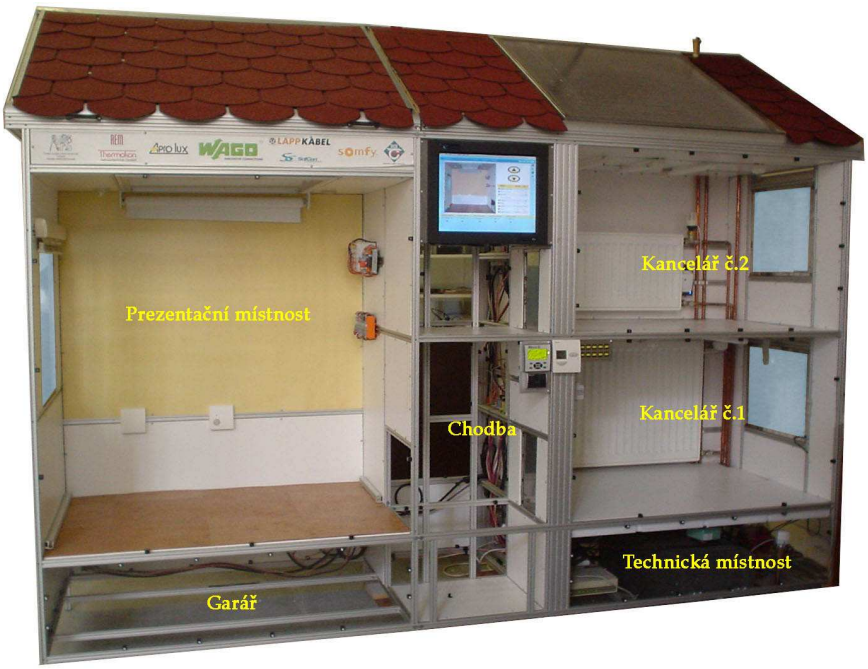
Tabulka 4 - Položky a hodnoty nabídky parametr

5. Model domovní automatizace

Model administrativní budovy se v současné době staví na katedře Řídicí techniky v Praze na Karlově náměstí. Model byl navržen jako dvoupatrová administrativní budova s půdou, sklepem a chodbou. Obsahuje prezentační místnost, dvě kanceláře, technickou místnost, garáž, dva půdní prostory a chodbu s výtahovou šachtou. Model je rozdělen na rozebíratelné části z důvodu potřeby prezentace modelu na výstavách.

Hlavní technologie v budově je LonWorks, DALI[6] a EnOcean. DALI je moderní technologie pro ovládání inteligentních světel. Tento mezinárodní standard (IEC 60929) umožňuje návrh a řízení decentralizovaných systémů. V budovách je používán stále častěji místo klasických zapojení.

[6] DALI – Digital Addressable Lightning Interface



Obrázek 8 - Model administrativní budovy

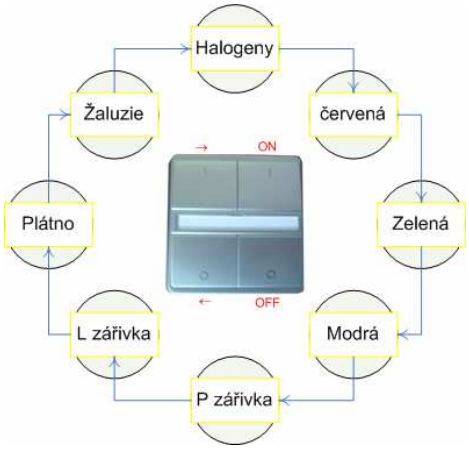
EnOcean je bezdrátová radiová technologie pracující na frekvenci 868.3 MHz. Cílem této technologie je používání alternativních zdrojů energie namísto baterií.

Pro realizaci byl vybrán stavebnicový systém Item, který tvoří eloxované hliníkové profily s výplněmi z tvrzeného PVC. Stavebnice zaručuje flexibilitu pro změny na modelu.

5.1. Prezentační místnost

Tato místnost je největší místností modelu a je umístěna v jeho levé části. V místnosti je nainstalováno zářivkové osvětlení, které je rozdělené na pravou a levou část, z nichž každá obsahuje dvě kompaktní zářivky. Dále jsou umístěny RGB LED panely pro barevné světelné scény v místnosti. Dalšími umístěnými zařízeními jsou bodové halogenové žárovky, snímače osvětlení pro místnost a pro plátno, senzor teploty místnosti EnOcean, senzor pohybu, elektricky ovladatelná žaluzie na okně a promítací plátno. Řídicí jednotkou této místnosti je programovatelný logický automat Wago 750-819 s komunikačním rozhraním LonWorks. K tomuto PLC jsou také připojeny dva speciální moduly DALI a EnOcean, která zajišťují potřebný interface mezi těmito technologiemi.

Na obrázku 9 je čtyř-tlačítko EnOcean, využívající stisku k vytvoření dostatečného množství energie k odeslání informace. Energie je získávána z piezo-elementů umístěných pod jednotlivými tlačítky. Výkon vysílačů této technologie je 10mW. Jejich minimální dosah je v budovách od 30m.



Obrázek 9a - Tlačítko EnOcean

Obrázek 9b - Funkce tlačítka EnOcean

Ovládání místnosti je zajištěno tímto radiovým čtyř-tlačítkem EnOcean. Pravé dvou-tlačítko přepíná mezi jednotlivými prvky v místnosti. Levé dvou-tlačítko ovládá vybraný prvek.

5.2. Kancelář č.1

Obrázek 10 - Kancelář č.1

Tato místnost se nachází v pravé části modelu dole nad Technickou místností. V místnosti je radiátor, otevíratelné okno, stahovatelná roleta, analogově řízená světla, senzor teploty místnosti a senzor intenzity osvětlení. Jako řídicí prvky jsou nainstalovány moduly DESIGO RX společnosti Siemens. Jsou zde dva hlavní moduly s dvěma přídavnými moduly. V prvním případě se jedná o modul RXC31.1 s přídavným modulem RXC40.1. V druhém případě se jedná o modul RXC30.1 a dva moduly RXC41.1.

5.3. Kancelář č.2

Obrázek 11 - Kancelář č.2

Tato kancelář je umístěna v druhém patře nad Kanceláří č.1. Je zde nainstalován radiátor a místnost je tepelně izolována polystyrénem. Osvětlení je realizováno pomocí dvou DALI světel, z nichž každé obsahuje dvě kompaktní zářivky. Místnost má dále také otevíratelné okno se stahovatelnými roletami. Dalším prvkem v místnosti je regulátor termohlavice radiátoru. Jako řídicí prvek je nainstalován softwarový logický automat WizPLC, který se sítí LON komunikuje pomocí OPC serveru.

5.4. Technická místnost

Technická místnost se nachází v pravé části modelu v přízemí. Je zde umístěn vytápěcí systém a jeho řídicí prvky. Dále je zde router L-IP a víceportový L-Switch. Zařízení L-IP slouží jako síťový interface a umožňuje komunikaci se sítí LON pomocí TCP/IP protokolu. Dále jsou zde zdroje napětí 24V jak stejnosměrného, tak střídavého.

5.5. Garáž

Garáž je ve fázi výstavby a nachází se v levé přízemní části modelu.

5.6. Chodba

Chodba se nachází ve střední části modelu mezi všemi místnostmi. Má dvě patra a obsahuje výtahovou šachtu ve které je umístěn výtah. Výtah byl realizován v rámci semestrální práce panem Josefem Veseckým avšak v době ukončování této práce nebyl zcela dokončen.

6. Wizcon Supervisor - Wizcon for Windows and Internet

Wizcon for Windows and Internet je program spadající pod balík programů Wizcon Supervisor (dříve Axeda Supervisor). Umožňují real-time i historické monitorování informací z budov jako jsou např. tovární haly, obchodní domy až po prezentační místnosti. Umožňují plnou SCADA/HMI[7] podporu na počítačích běžících na 32-bitových platformách Windows s integrovanou schopností prezentovat stejné informace na jakémkoliv webovém prohlížeči, vybaveném pluginem Java.

Uživatelé mohou vytvářet aplikace běžící současně na dvou úrovních:

- Wizcon SCADA aplikace běžící na Windows NT a XP. tyto aplikace mohou být prohlíženy na jakémkoliv standardním SCADA počítači s instalovaným OS Windows.

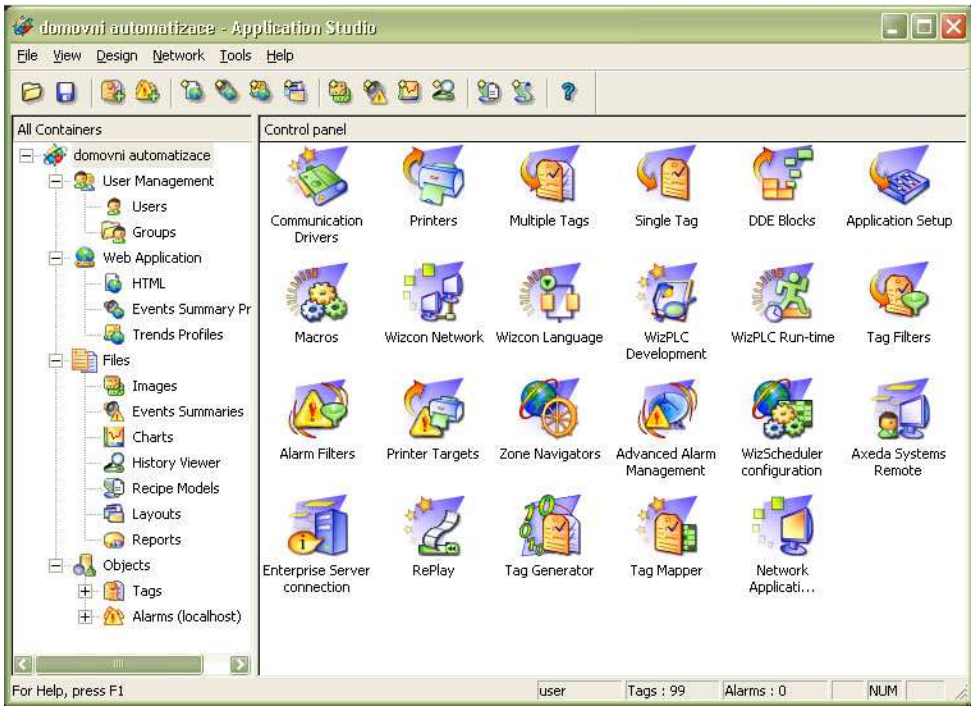
- Wizcon web SCADA aplikace běžící na standardních Windows NT a XP webových serverech. Tyto aplikace jsou založené na Java a mohou být prohlíženy na jakémkoliv webovém prohlížeči, který Java podporuje.

Vývojové prostředí Wizcon umožňuje uživateli sestavit Real-Time Databázi (RTDB) pro vytvářené aplikace. Tato databáze se skládá z definicí tagů[8] a alarmů[9]. Dále se definuje komunikační ovladač, a může se pokračovat sestavením HMI rozhraní, obsahujícím obrázky, grafy a seznamy událostí. Uživatel dále může tyto aplikace spouštět na operátorských SCADA stanicích s operačním systémem Windows nebo je publikovat na internetu prostřednictvím konverze aplikace do jazyku HTML a java aplettů. Webově založené aplikace umožňují monitorování sítě prostřednictvím Wizcon serveru.

[7] **SCADA** – Supervisory Control And Data Acquisition – Centrální systém, který monitoruje a řídí kompletní síť přístrojů a senzorů. Typickým představitelem je síť s distribuovanou inteligencí.
HMI – Human Machine Interfaces - uživatelsky přívětivé řídící rozhraní automatizačního systému
[8] **Tag** – vnitřní proměnná Wizconu, reprezentuje aktuální hodnotu přístroje nebo snímače připojeném na automatizační síť.
[9] **Alarm** – při překročení určité nastavitelné úrovně tagu se automaticky spustí alarm, např. zobrazení pop-up okna nebo spuštění makra

6.1. Hlavní okno

Tato nabídka je hlavní nabídkou programu Wizcon. Této sekci se také nazývá „All containers“. Zde je k dispozici kompletní nastavení aplikace a jsou zde umístěny všechny nástroje potřebné k vytváření aplikace. K této sekci mohou mít povolen řístup pouze uživatelé, kteží se nalogují s oprávněnám jménem a heslem.
Následuje popis hlavních částí programu:



Obrázek 12 - Programovací prostředí Wizcon – *All Containers section*

Popis hlavních částí aplikace Wizcon (viz obrázek 12)

- **Communication Drivers** (komunikační ovladače)
- **Macros** (makra)
- **Users** (uživatelé)
- **HTML** (internetové stránky)
- **Images** (řídicí vizualizace)
- **Event Summaries** (seznamy událostí)
- **Charts** (grafy)
- **Tags** (vnitřní proměnné)
- **Alarms** (oznámení o mimořádných událostech

6.1.1. Communication Drivers

Komunikační ovladače umožňují komunikaci s externími zařízeními připojenými do sítě. Tyto ovladače jsou oddělené programové soubory, tzv. knihovny, a jsou nainstalované spolu s aplikací. Na výběr je mnoho typů ovladačů, navíc také pro simulační účely tzv. Randomize driver. Tento ovladač umožňuje zvolení rozsahu tagu a následně generuje hodnotu tagu v námi definovaném rozsahu.

Námi zvolený ovladač OPC serveru OPC Data Access Client (VPIWNOPC) komunikuje s OPC serverem Iplongate a Wizconem. a předává mu hodnoty do námi nadefinovaných tagů (o tagu viz níže).

6.1.2. Macros

Makra jsou předdefinované akce, příkazy nebo programy, které spustí uživatel kliknutím na trigger, který na ně odkazuje. Může je také spustit alarm nebo stisk klávesy nebo kombinace kláves. Trigger je vlastnost objektu. Objekt s takovouto vlastností je tlačítko.

Definovat makra je výhodné zejména pokud děláme komplexní aplikaci která je uživatelsky přívětivá a máme nastavené alarmy při překročení limitních hodnot tagů. Při překročení limitních hodnot tagů se automaticky spustí makra která provedou přesně stanovenou funkci. Tyto makra mohou např. informovat uživatele pop-up oknem[10] nebo spustí námi předefinovaný sled příkazů.

6.1.3. Users

Uživatelé aplikace se nastavují v této nabídce. Aplikace zároveň umožňuje nastavit různá přístupová práva jednotlivým uživatelům. Lze nastavit přístupová práva k tagům, k makrům a dokonce i k položkám menu programu. O definovaném uživateli můžeme mimo to ukládat i informace jako je jméno, adresa a kontakt. Uvedený kontakt může být použit přímo AAM servisní službou, která se stará v případě nestandardních podmínek na stanici o real-time informování uživatelů na e-mail, mobilní telefon, fax či pager. AAM servisní služba je komponentou prostředí Wizcon.

Lze definovat i skupiny uživatelů. Členové této skupiny budou mají stejná přístupová práva jako skupina ke které patří. Jeden uživatel může být zároveň členem několika skupin.

Nastavení přístupových práv je výhodné nejen při používání programu přímo na pracovišti, ale např. při umístění aplikace na internet. Na internetu by každý

[10] **Pop-up okno** je druh okna ve Windows. Automaticky se maximalizuje při nějaké situaci.

uživatel který by se podíval na příslušné stránky měl možnost ovlivňovat hodnoty tagů nebo měnit nastavení připojeného automatizačního systému. Tomu lze zamezit např. tak, že defaultnímu uživateli který je automaticky nalogován po spuštění programu určíme přístupová práva pouze pro čtení. Je nutné nadefinovat další uživatele jako administrátory systému, jejihž účet je chráněn bezpečnostním heslem a kteří mají nastavené přístupová práva tak aby mohli ovlivňovat dění na připojeném automatizačním systému.

6.1.4. HTML

Konverze aplikace do HTML formátu s Java applety[11].

6.1.5. Images

Hlavní část programu. Zde se vytváří HMI grafická vizualizace (dále jen vizualizace) - image. Image je dynamická grafická reprezentace řízeného automatizačního procesu. V řízeném procesu jsou tagy reprezentovány grafickým objektem kde každý objekt reprezentuje určitou hodnotu tagu. Společně mohou zobrazovat dynamický obrázek pracovního procesu.

Pro vytváření vizualizace můžeme použít interních kreslicích nástrojů, které jsou standardní pro různé kreslicí programy nebo využít nainstalovaných knihoven s předpřipravenými nejpoužívanějšími objekty, tzv. *clustery*. Clustery jednoduše přetáhneme stylem drag & drop[12] do vizualizace. Clustery jsou přehledně uspořádané v několika knihovnách, pojmenovanoných podle objektů v ní se vyskytujících, např. klimatizace, budova, tlačítka atd. Lze také importovat obrázky typu bmp, jpg a jpeg.

Jakýkoliv objekt lze nastavit jako trigger. Trigger[13] je uživatelem definovatelná vlastnost objektu. Objekt s touto vlastností je tlačítkem, které přímo zapisuje dané hodnoty do tagů a jejich prostřednictvím přímo do sítě LON. Trigger také může aktivovat makro. Program umožňuje simulaci hodnot tagů, nezávislou na připojeném automatizačním systému. Simulace hodnot se osvědčí zejména při ladění grafické stránky vizualizace, kde vzhled objektu je přímo závislý právě na jeho hodnotě.

Jednotlivým objektům lze přiřazovat dynamické vlastnosti. Objekty s dynamickými vlastnostmi reagují na aktuální hodnoty tagů, tzn. že se mění

[11] **Applet** je softwarový komponent který běží v kontextu jiného programu, v tomto případě se jedná o webový prohlížeč. Java applet obvykle vykonává velmi úzkou funkci, která není prováděna nezávisle.

[12] **drag & drop** (angl.) = táhni a pusť; styl kopírování ve windows; myší uchopíme objekt, který jednoduše přetáhneme tam, kam ho chceme zkopírovat

[13] **trigger** (angl.) = spouštěč

grafická podoba řízeného procesu. Spolu s použitými zapojenými senzory do sítě LON můžeme vizualizaci nastavit takové parametry, že vzdálení uživatelé[14] vidí aktuální dění na pracovišti. Mezi dynamické vlastnosti patří zvětšení, zmenšení, rotace, vyplnění barvou, zobrazení, skrytí, blikání atd. Vizualizaci lze individuálně přibližovat či oddalovat, může se skládat až z 64 vrstev. Jednu vrstvu lze rozdělit na libovolné množství zón a mezi nimi využitím interní funkce „go to zone[15]“ libovolně přepínat. Operátoři mohou přistupovat pouze k vrstvám, ke kterým mají povolený přístup.

6.1.6. Event Summaries

Event Summaries jsou seznamy událostí zobrazující dosažené hodnoty tagů v závislosti na uživatelově nastavení. Uživatel může nastavit filtry k zobrazení alarmů, které jsou jen z některé zóny, důležitosti a dosahují určité hodnoty atd. Tyto alarmy zde mohou být také tříděny. Zobrazeným hodnotám lze nastavit různou barvu pozadí nebo písma, což zvyšuje přehlednost pohybujícího se seznamu. Event Summaries lze kombinovat s vizualizací, ve které je umístěn odkaz. Viditelnost systémové nabídky pro různé uživatele je ovlivnitelná v sekci *Users*.

6.1.7. Charts

Grafy. V této části lze zobrazit historické nebo online hodnoty tagů. Jednotlivým grafům lze nastavovat barvu pozadí nebo barvu křivky. Můžeme nastavit grid a časové osy. Při spuštění grafu lze nastavit zobrazení historických hodnot až několik dní zpětně. Grafy lze kombinovat s vizualizací, ve které je umístěn odkaz na graf. Viditelnost systémové nabídky pro různé uživatele je ovlivnitelná v sekci *Users*.

6.1.8. Tags

Tagy jsou vnitřní proměnné Wizconu, jejichž hodnoty se mění dle toho, jak jsou čteny ze sítě LON nebo naopak posílány do LONu. Existuje několik různých druhů tagů a jejich hodnoty lze upravovat ať už vzájemným ovlivňováním nebo kompenzací konstantou.

Hodnoty tagů mohou být načítány a nahrávány do souborů, které obsahují historická data specifikovaná uživatelem. Tagy mohou být dále posílány externí aplikaci přes rozhraní DDE. Tag může být také zamknut nebo odemknut jen v určitý předdefinovaný čas.

---

[14] **vzdálení uživatelé** – uživatelé využívající vzdáleného připojení k automatizovanému systému, např. uživatelé na internetu

[15] **go to zone** (angl.) = jdi do zóny

Druhy tagů:

- **Systémové** – základní tagy prostředí Axeda. Jsou to speciální tagy vztažené k počítačové stanici, na kterém je spuštěná Axeda. Mezi ně patří např. aktuální čas, datum, velikost volné paměti, volné místo na disku apod.
- **RePlay tagy** – tagy ve kterých jsou uložena historická data. Spuštěný RePlay modul zobrazuje chronologicky v nastaveném časovém rozsahu historické dění na pracovišti,
- **Uživatelské tagy**, nastavitelné uživatelem; jejich zdroje:
  - **PLC** – tyto tagy jsou asociovány s externími moduly. Aplikace hodnoty těchto tagů periodicky načítá pomocí komunikačního ovladače,
  - **Compound** – lineární kalkulace jiných tagů,
  - **Dummy** – reprezentace vnitřních proměnných. Dummy tagy jsou obnovovány uživatelským vstupem nebo měněny ostatními moduly aplikace.

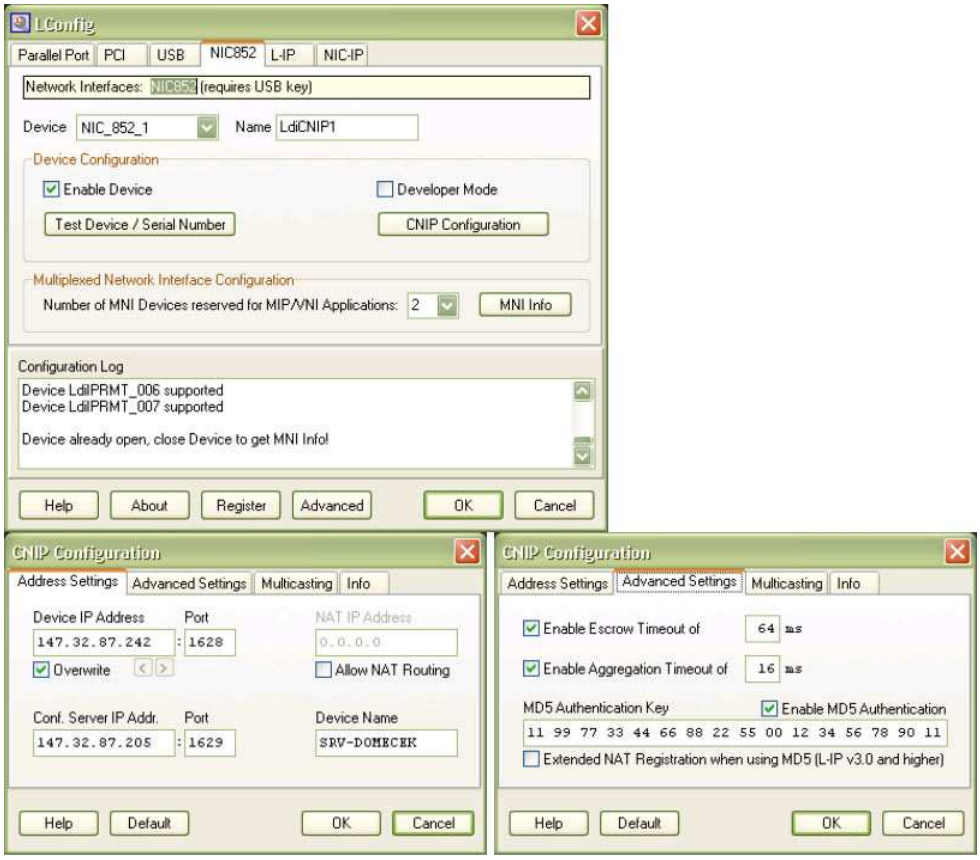
6.1.9. Alarms

Alarmy jsou nastavitelné zprávy, které upozorňují operátora na výjimečné hodnoty na pracovišti. Alarmy mohou být zaslány do seznamu událostí, pop-up okna nebo být vytisknuty. Také mohou být tříděny dle hierarchie.

6.2. Postup sestavení nové vizualizace pro ovládání budovy

6.2.1. Kontrola nastavení Lconfig

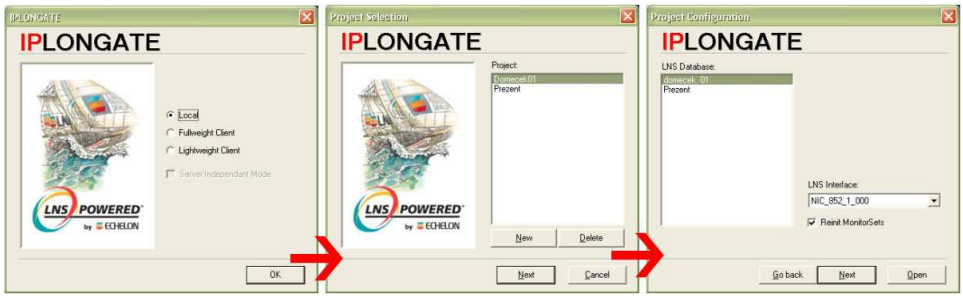
Před vytvořením nové aplikace je nutné zkontrolovat nastavení bez kterých by aplikace nefungovala správně. Důsledkem nefunkční komunikace mezi spuštěnými softwarovými servery by byla nemožnost zápisu a čtení hodnot SNVT proměnných na LONu reprezentovaných tagy ve Wizconu. **Toto nastavení je třeba provést vždy potom kdy je na domečkovském PC vytvořen nový uživatel OS Windows!** Je nutné kliknout pravým tlačítkem myši na lištu nabídky *Start* ve Windows na *Legacy Driver* a zvolit podpoložku *LConfig*, dále zvolit kartu *NIC852* a poté kliknout na *CNIP Configuration*. Do příslušných políček se vyplní IP adresa počítače a IP adresa konfiguračního serveru. IP adresa počítače je „147.32.87.254“ a IP adresa konfiguračního serveru je „147.32.87.205“. Dále se vyplní MD5 autentifikační klíč. Hodnota klíče MD5 je „11 99 77 33 44 66 88 22 55 00 12 34 56 78 90 11“. Postup nastavení je vyznačen na následujících obrázcích:



Obrázek 13 - Loytec - Nastavení Lconfig

6.2.2. Spuštění OPC serveru

Před spuštěním prostředí Axeda se musí spustit nejprve nainstalovaný externí server OPC Iplongate který přes LNS databázi a definovaný vstupní bod sítě vstupuje do sítě LON a přeposílá vzájemné hodnoty proměnných. Spuštění serveru OPC se provede kliknutím na ikonku *Iplongate* na pracovní ploše Windows. Musí být vybrána LNS databáze *Domecek01* a vstupní hardwarový bod sítě (LNS interface) je *NIC_852_000*. **Program Iplongate je nutné dále spouštět vždy předtím než je spuštěn Wizcon!**



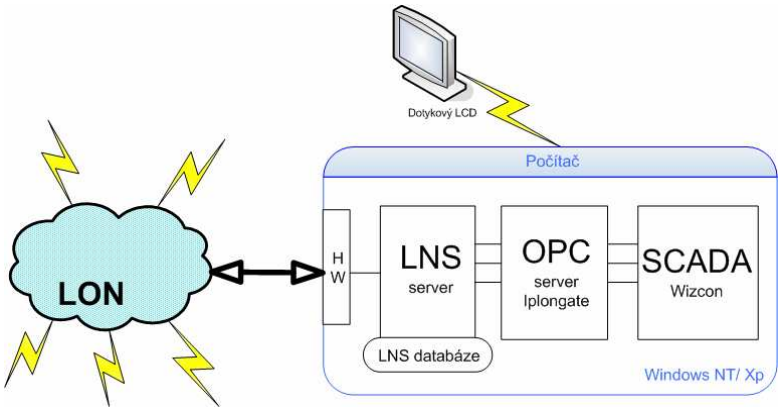
Obrázek 14 - Spuštění Iplongate

6.2.3. Založení nové aplikace

Po spuštění programu Wizcon ikonkou na ploše se zobrazí okno ve kterém se musí zadat jméno nové aplikace a umístění adresáře. Po prvním spuštění se objeví dialogové okno, ve kterém program žádá o vložení systémových tagů. Na výběr jsou možnosti „Vložit hned“ a „vložit později“. Doporučuji zvolit vložení hned.

6.2.4. Definice komunikačních ovladačů

Při spuštění nové aplikace je nejprve nutné nadefinovat potřebné komunikační ovladače. Komunikační ovladače jsou softwarová rozhraní, která umožňují komunikaci mezi prostředím Wizconu a sítí LON. Komunikace se děje prostřednictvím programu IPLongate, LNS databáze, a hardwarovým rozhraním. IPLongate je softwarový OPC server, nainstalovaný na PC v domečku, který se stará o zprostředkování dat mezi LNS databází a programovým prostředím Wizconu. LNS databáze je virtuálně namapovaná síť LON, vytvořená pomocí programu LonMaker, v klasickém prostředí MS Visio. Protože Wizcon komunikuje přímo s OPC serverem, je ho nutné nadefinovat jako používaný komunikační ovladač v programu. Proto je také nutné spustit tento server před spuštěním prostředí Axeda Wizcon, aby komunikace mezi LonWorks a řídicí vizualizací probíhala bez jakýchkoliv problémů. Komunikace mezi PC v domečku a sítí LonWorks je naznačena na následujícím obrázku.



Obrázek 15 - Schéma komunikace vizualizace Wizcon se sítí LonWorks

Postup nastavení komunikačního ovladače OPC*:*

V hlavní nabídce Wizconu je nabídka *Communication Drivers*, ve které se stiskne pravé tlačítko myši. V zobrazené podnabídce se klikne na *Add* a z příslušné nabídky se vybere *OPC Data Access Client (VPIWNOPC)*.

Obrázek 16 - Wizcon - Nastavení komunikačních ovladačů

Po zadání logického jména driveru, což znamená naše pojmenování, už není nutné žádné nastavené hodnoty měnit a instalace driveru se může dokončit.

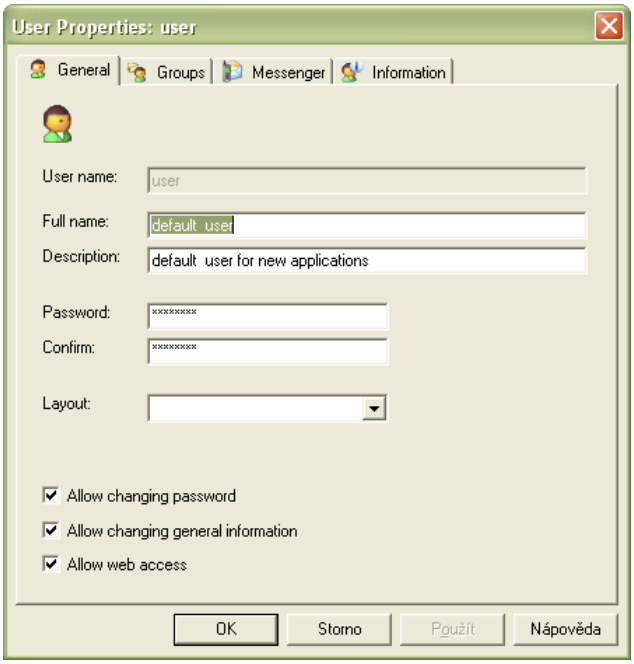
6.2.5. Nastavení uživatelů a uživatelských skupin

Nastavení uživatelů by mělo následovat ihned po nastavení komunikačních ovladačů. Toto doporučuji provést zde na začátku neboť každá úroveň návrhu aplikace se může opírat o uživatelskou autorizaci. Ušetří to práci v pozdějších fázích projektu. Každý uživatel může mít různá práva pro přístup jak k tagům tak k celému software.

Seznam komponent, ke kterým může být limitovaný přístup:

- Menu a položky menu
- zápis do tagů
- aktivace maker
- grafické elementy vrstev ve vizualizaci
- oznámení alarmu

Pokud je v hlavní nabídce kliknuto na ikonku *Users* je zobrazeno následující okno:



Obrázek 17 - Wizcon - definování nového uživatele

Zadá se jméno, uživatelské jméno nového uživatele a přístupové heslo. V zaškrtávacích políčkách se nastaví povolení změny hesla, povolení změny informací o uživateli a povolení webového přístupu (viz obr. 19).

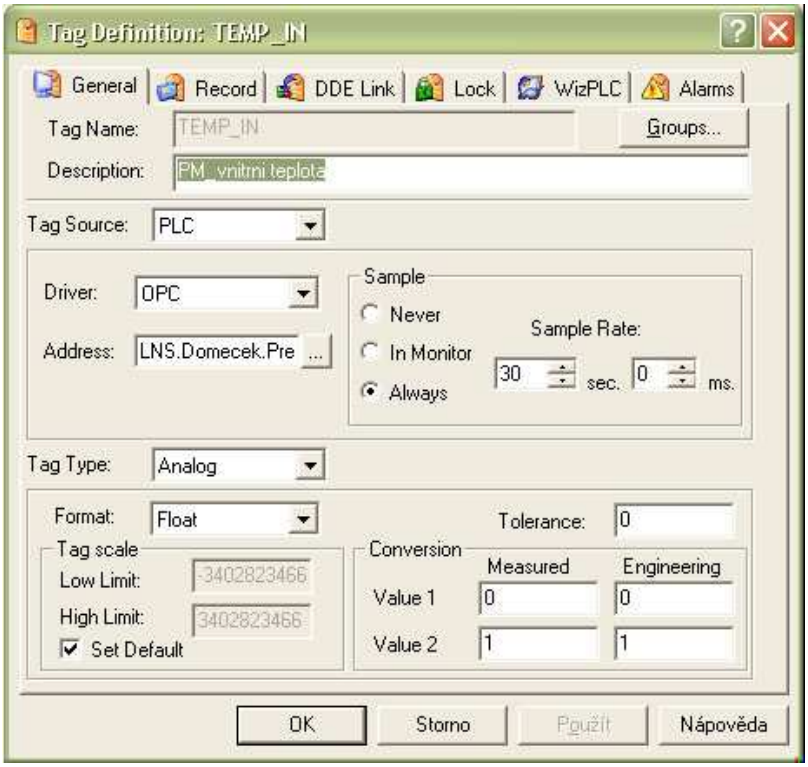
Na dalších záložkách se může nastavit členství v nadefinovaných skupinách, messenger[16] neboli AAM kurýr zpráv, a naposled také detailní informace o uživateli, jako je jméno, adresa atd.

K defaultní skupině Administrators se založí skupina hostů Quests. kteří budou mít k aplikaci též přístup, avšak nebude jim povolena možnost měnit stav objektů v budově, což bude výhodné zejména až budou vytvořeny webové stránky, a výsledná vizualizace bude online na internetu. Nastavení přístupovým práv k tagům se děje v následujícím bodě (při kliknutí na ikonku *Groups* na obrázku 18).

6.2.6. Definice tagů

Dalším bodem, který by měl následovat, je vlastní definice tagů. Tagy lze nadefinovat až po vytvoření grafické vizualizace. Avšak nastavení tagů v tomto bodě velice usnadní ladění později vytvořené vizualizace. Dialogového okna tagu se po kliknutí na záložku *Tags* v hlavní nabídce a po zvolení podnabídky *Add tag...*

[16] **Messenger** – kurýr zpráv – speciální nástroj umožňující zasílat informace o aktuálním stavu aplikace na e-mail, fax nebo pager.



Obrázek 18 - Wizcon - definice tagu

V záložce *General* se nastaví jméno tagu a popis. Je vhodné popis (*Description*) vyplnit z důvodu pozdějšího snadnějšího orientování ve výpisu všech tagů.

Existují tři typy zdrojů tagu *Tag source* a to jsou: PLC, Compound a Dummy. Tag source PLC se používá při vnějším zdroji, např. vnější OPC server. Toto je případ domečku. Tag source Compound je vypočtený tag závislý na ostatních. Tag source Dummy znamená jednoduchý tag který může zastávat funkci pomocného tagu. Nabývá např. hodnot jedna nebo nula a podle toho jsou ovládány ostatní prvky vizualizace.

Aby byli nalezeny všechny moduly napojené na Lonworks, jako zdroj tagu musí být zvolen Tag source PLC, komunikační ovladač (*Driver*) bude OPC. Kliknutím na tlačítko „…“ se zobrazí okno ve kterém se najde příslušný nód na LonWorks namapovaný v LNS databázi.

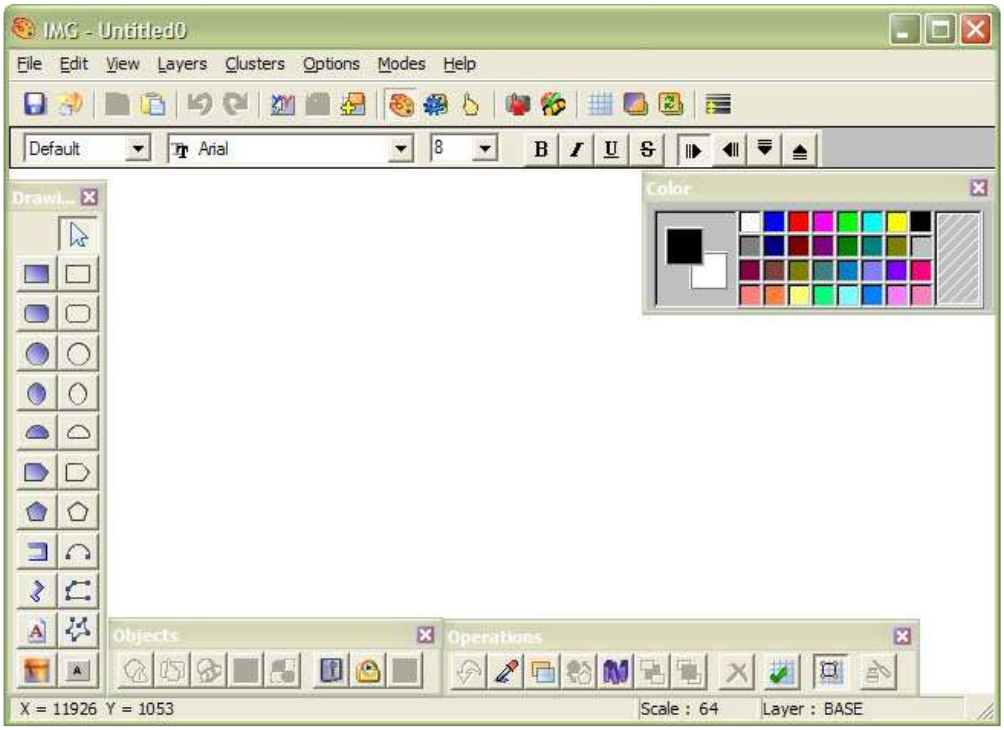
V části *Sample* se vyplňuje vzorkování tagu. *Never* je doporučeno používat pouze pro vstupní hodnoty, kdy se hodnota tagu sama neaktualizuje, ale děje se tak při kliknutí na nějaký objekt, který umožňuje uživatelský vstup. Položka *Always* což znamená vždy obnovovat se zatrhne v případě načítání např. ze senzoru teploty nebo z jakéhokoliv senzoru. *Sample Rate* čili vzorkování se zvolí přiměřené danému tagu. Např. pro teplotní čidlo se nemusí volit obnovování každých 100ms, ale stačí třeba každých 60sec, záleží na konkrétní aplikaci později vytvořené vizualizace.

V části *Groups* lze nastavit přístupová práva k tagu pro určité uživatele nebo pro skupiny uživatelů.

6.2.7. Vytvoření Image

Grafická vizualizace, neboli Image, je hlavní část programu ve Wizconu. Jejím prostřednictvím může být řízen fyzikální objekt na síti LonWorks. Řízení může být intuitivní, grafika může být dynamicky měnitelná, záleží vždy na konkrétním projektu a na přístupu programátora.

Hlavní okno se zobrazí po kliknutí na *Images* v hlavní sekci Wizconu. Okno návrhu je složené z několika panelů a nabídek, jak je vidět z následujícího obrázku:



Obrázek 19 - Wizcon - hlavní okno návrhu grafické vizualizace

Existují dva módy spuštěné vizualizace:

- ***Edit*** – tento mód se používá pro návrh a editaci vizualizace
- ***Trigger On*** – spuštěním tohoto módu se objekty, které jsou definovány jako triggery, aktivují a mohou být použity pro řízení procesu.

Seznam hlavních paletek přístupných v módu *Edit*:

- Drawings
- Color
- Objects
- Operations

Paletka *Drawings* obsahuje hlavní objekty, které se mohou umístit do Image. Objekty jsou čtverec/obdélník, čtverec/obdélník se zaoblenými rohy, kruh, elipsa, část kruhu, ortogonální polygon, polygon. Existují dva druhy těchto objektů a to buď vyplněné barvou popředí, nebo nevyplněné. Dalšími objekty, které lze kreslit jsou ortogonální roura, roura, ortogonální čára, čára a neuzavřená část kruhu. Posledními objekty jsou tlačítko, text a obrázek.

Všem těmto uvedeným objektům lze nastavovat vlastnosti jako je barva apod. a také trigger a dynamické vlastnosti. Navíc se zobrazením rozšiřující nabídky (pravé tlačítko myši) u jakéhokoliv objektu a kliknutím na *Group* mohou sdružovat do skupin a položkou *Ungroup* se mohou ze skupiny zase vyčleňovat. Výhodou toho je, že změnou jednoho objektu ve skupině se změní všechny ostatní, takže není nutné vlastnosti nastavovat u každého objektu zvlášť.

Zajímavým objektem je Text. Na obrázku 19 je to ikonka „červené A“ v paletce. Textových polí může být několik druhů. Nejpoužívanějším textovým polem je typ *Tag Value* a *Text Table*. *Tag Value* reprezentuje hodnotu tagu, a to dekadickou, hexadecimální nebo string. Je zde možnost nastavení zobrazení počtu platných míst před a za desetinou čárkou. Těchto platných číslic lze nastavit shodně 1 až 20 v obou případech. Dále je zde možnost nastavení zobrazování a nebo skrytí znaku + v případech kladné hodnoty a dále nastavení zarovnání (vpravo, ve středu a nebo vlevo). Stručně řečeno objekt *Text* typu *Tag Value* zobrazuje hodnotu tagu.

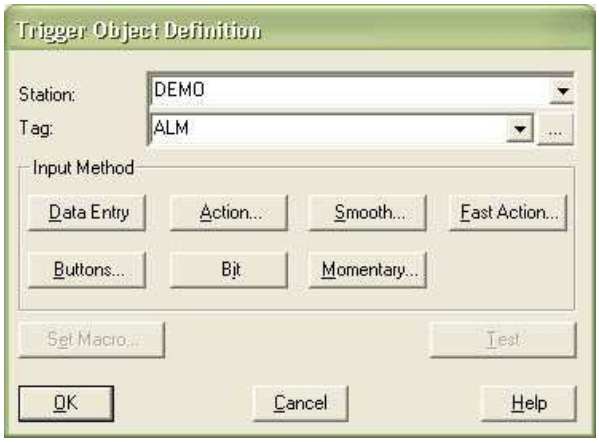
Objekt *Text* typu *Text Table* zobrazuje pouze zapsané číslo nebo znak. Samozřejmostí je u textového pole obou druhů nastavení velikosti písma, a to lze nastavit v systémovém menu *Images* > *View* > *Fonts*.

Obrázky mohou být vloženy typu bmp, jpg nebo jpeg. Jistou nevýhodou je nemožnost importu obrázku typu gif u kterého je výhodou že nemá určenou barvu pozadí, což je výhodné pro návrh vzhledu celého řídicího procesu.

Paletka *Color* je paletka barev známá z jiných programů.

V paletce *Objects* jsou nejhlavnější funkce a některé speciální objekty. Kliknutím na *Alarm Definition* se nastavuje akce alarmu, která se má provézt při nestandardních podmínkách na pracovišti.

Pomoví ikonky *Trigger Definition* se přiřazuje vlastnost býti Triggerem nějakému objektu, který se pak chová jako tlačítko. Tato ikonka je jednou z nejdůležitějších, neboť pomocí této funkce se děje softwarové propojení mezi vizualizací a sítí LonWorks. Možnosti nastavení *Trigger Definition* jsou vidět v následujícím obrázku:



Obrázek 20 - Možnosti nastavení Trigger Definition

Tlačítko *Data Entry* se používá při posílání konkrétní hodnoty nebo znaku (string) pomocí tagu do LonWorks. Uživatel bude zadávat tuto hodnotu při poklepání na objekt s touto vlastností. Tlačítko *Action* se používá pro nastavení pevně definované akce, např. spuštění makra nebo pro přechod do jiné zóny. Tlačítko *Fast Action* slouží k nastavení spouštění akcí, které jsou částí programového balíku Wizcon a byly spolu s ním nainstalovány. Jedná se o užitečné funkce typu „Jdi do určené zóny“ , „otevři graf“ , „jdi na URL“, „otevři obrázek“ apod.

Tlačítko *Dynamic Definition* nastavuje dynamické grafické akce závislé na aktuální hodnotě tagu. Mezi tyto akce patří, zobrazení/ skrytí objektu, jeho otočení, vylnění barvou, blikání atd. Tlačítko *Cluster Definition* slouží k přidání vybraného objektu do interní databáze předpřipravených grafických objektů. Databáze Wizconu obsahuje desítky těchto objektů rozdělených do několika tematických podskupin, které lze ve vizualizaci rovnou použít. Tlačítkem *Group* lze vybrané objekty přidat do skupiny.

Nabídka *Operations* obsahuje také několik možností co lze s vybraným objektem dělat. Patří sem tlačítko *Rotate* , kterým lze vybraný objekt otáčet dokola. Dalším tlačítkem je *Cluster library*, které otevře knihovnu Clusterů. Objekty lze do vizualizace přenášet metodou „Drag&Drop” tzn. uchopením myší a přesunutím. Dalšími používanými tlačítky jsou *Send to Back* a *Send to Front* - umístění objektu na pozadí nebo na popředí. Tyto tlačítka nacházejí uplatnění v případě několikavrstvé vizualizace, kde jsou objekty umístěny přes sebe.

Dalšími důležitými tlačítky jsou *Grid* a *Snap to Grid* , která zobrazují a uchycují objekty do virtuální mřížky, tzv. gridu.

Postupným umisťováním objektů z paletky Drawings, z knihovny Clusterů a importováním obrázků se vytvoří grafická podoba vizualizace. Poté se objektům nastaví vlastnost Trigger, která ovlivňuje dění na LonWorks. Dynamické vlastnosti

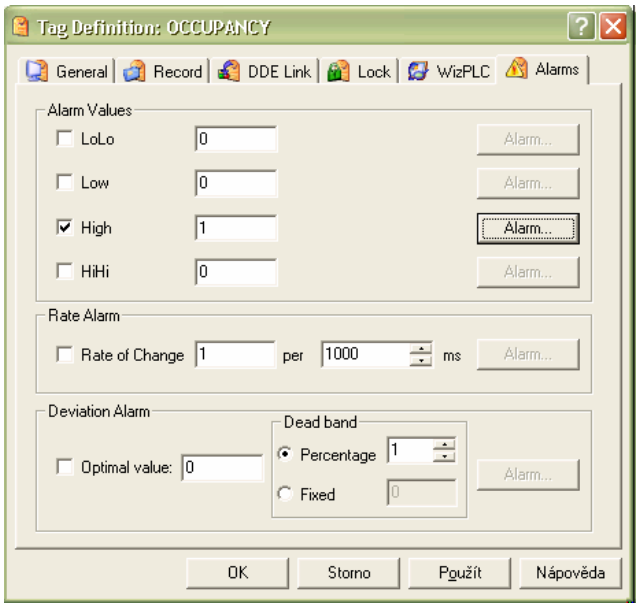
se definují v posledních fázích návrhu, kde využijeme simulaci hodnot tagů v systémové nabídce *Options* > *Simulate*.

6.2.8. Další možnosti vytvořené aplikace

Po vytvoření aplikace se nastaví grafy pro jednotlivé tagy, seznamy událostí, alarmy a nakonec se celá aplikace jednoduše exportuje do HTML formátu pomocí automatické konverze ve Wizconu.

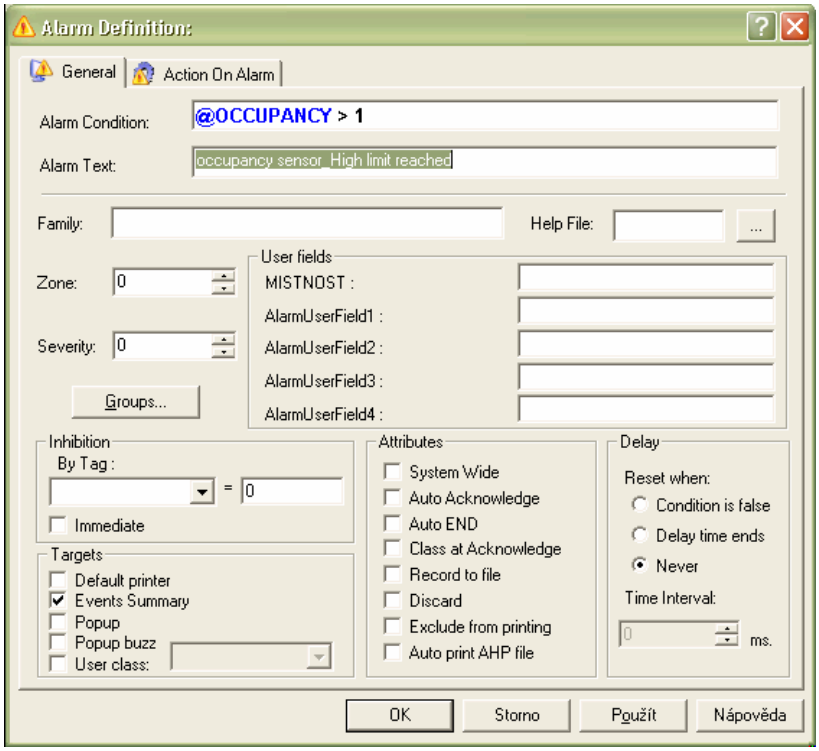
Vytvoření nového grafu se provede tak, že v hlavním okně vizualizace klepneme na ikonku *Charts* a postupujeme systematickým návrhem dle nabídky *Setup*, kde nastavíme tag, který se bude monitorovat, rozlišení časové osy a mezní hodnoty velikosti osy *y*. Dále se může nastavit zobrazení *grid*u, které je možno využít k přesnějšímu odečítání hodnot z grafu. Samozřejmostí je možnost nastavení barev.

Vytvoření alarmu se provádí v podmenu *Tags*, kde se klikne na tag, který bude monitorován v seznamu událostí. V editačním okně tagu, vyvolaném pravým tlačítkem myši a zvolením M*odidy Tag*, je karta *Alarms*. Na této kartě lze nastavovat různé akce které se spustí při určité hodnotě tagu. Okna jsou zobrazena na následujících obrázcích:



Obrázek 21 - Editace tagu - nastavení alarmu

Kliknutím na *Alarms...* v okně pro editaci tagu (obr. 21) se vyvolá následující okno (obr. 22):

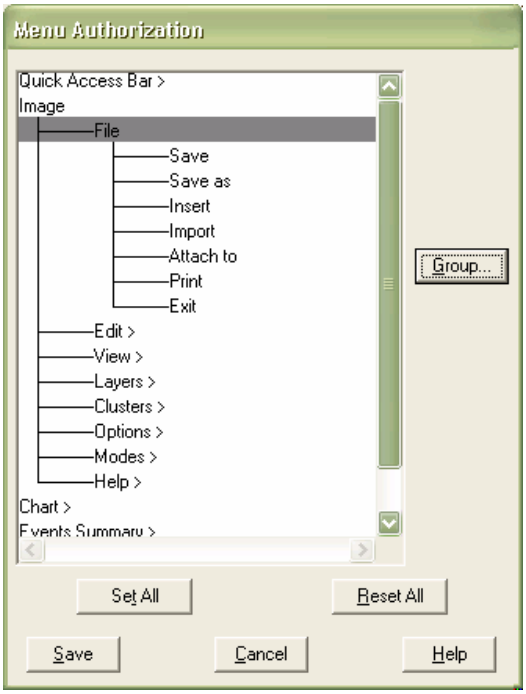


Obrázek 22 - Nastavení alarmu

V tomto okně lze upravit podmínku pro spuštění alarmu (viz. obr. 22). Dále lze alarm zacílit na tiskárnu, vypsat ho seznamu událostí event summaries, spustit popup okno apod. Dále lze zobrazit příslušnou zónu nebo sputit jiný image. Toto se dá nastavit na kartě nazvané *Action On Alarm*.

Vytvoření seznamu událostí se provede v hlavním okně Wizconu kliknutím na *Event Summaries* a vybráním položky *New Event Summary*. Druhou možností je zacílení alarmu na Events Summary položku (viz. obr. 22). V seznamu událostí lze upravovat barvy výpisu jednotlivých alarmů podle jejich důležitosti a podle druhu.

V posledním kroku se může nastavit jednoduché bezpečností opatření proti možnosti editaci jak jednotlivých částí programu (vizualizace samotné, grafu nebo seznamu událostí), tak celé vytvořené aplikace. Na následujícím obrázku je zobrazené menu, kde se nastavuje možnost přístup k jednotlivým systémovým nabídkám aplikace. Toto okno se vyvolá v hlavní sekci Wizconu, kliknutím na *Design> Authotization> Menu Items...* v systémovém menu okna. Přístupová práva se nastavují vybráním položky a kliknutím na tlačítko *Group...*



Obrázek 23 – Menu Authorization

Vytvoření internetových stránek se provede také v hlavním okně aplikace, kliknutím na *HTML* a zvolením *New HTML File*. Objeví se okno, kde se zatrhne co všechno je potřeba aby Wizcon vygeneroval – obrázkový prohlížeč, prohlížeč seznamu událostí nebo prohlížeč grafů. Stisknutím tlačítka *Generate* se automaticky vygeneruje HTML kód celé aplikace včetně appletů jazyka Java. HTML kód se poté může uploadovat na internetový server, kde může být prohlížen klasickým internetovým prohlížečem, který podporuje Java.

7. Závěr

Při realizaci této práce jsem se podrobně seznámil s vývojovým prostředím Wizcon for Windows and Internet, spadajícím pod balík programů Wizcon Supervisor společnosti Wizcon Systems, technologií LonWorks, snímačem otisků prstů M22(S)-ESA společnosti Moeller a řadou dalších softwarových produktů. Realizoval jsem grafickou vizualizaci pro ovládání inteligentní budovy přes dotykový LCD a pomocí internetu. Instaloval jsem snímač otisků prstů jako biometrický klíč pro vstup do kanceláře č.1.

Ovládání modelu administrativní budovy je zajištěno grafickou vizualizací. Vizualizaci jsme rozdělil na několik zón, kde každá zóna reprezentuje jednu místnost, nacházející se v budově. Do každé zóny jsem umístil hlavní panel, na

kterém jsou tlačítka pro přepínaní mezi jednotlivými místnostmi, zobrazený čas a jméno přihlášeného uživatele. V pravé horní straně každé zóny je umístěno tlačítko pro nalogování registrovaných uživatelů a nebo administrátorů systému, tlačítko pro zobrazení internetových stránek budovy, tlačítko pro zobrazení seznamu událostí v budově a tlačítko pro nápovědu ovládání. Z důvodu použitých různých technologií v budově a tedy různých rozhraní pro LonWorks je ovládání každé místnosti založené na jiném principu. Proto jsem nápovědu vytvořil pro každou místnost zvlášť. V místnostech kde je zpětná vazba ze senzorů je grafická stránka vizualizace dynamicky se měnící podle toho, jaké zařízení je právě zapínáno nebo vypínáno. Dále jsem na dolní část každé obrazovky umístil žlutou lištu kde jsou vypsané hodnoty všech senzorů umístěných v příslušné místnosti a také tlačítka pro zobrazení hodnot v grafu. Vizualizaci jsme testoval a upravil tak aby byla pro budoucí uživatele přívětivá a všechny odkazy a funkční tlačítka byly umístěny na místech kde je uživatel bude čekat. Ve vizualizaci je nastavené automatické nalogování uživatele *user*, který nevlastní přístupová práva pro změnu hodnot tagů a tímto způsobem je mu zabráněno v řízení modelu. Pouze uživatel který zadá své přihlašovací jméno a heslo smí ovládat budovu. Uplatnění se nachází zejména u dálkové správy budovy, kdy je tímto zabráněno každému uživateli, který vstoupí na internetové stránky budovy, v jejím řízení a zároveň v úpravě již vytvořené vizualizace. Přístupová jména a hesla k vytvořeným uživatelským účtům ve Wizconu jsou na PC v domečku na adrese C:\galbam1\x.txt a na CD dodaném s touto prací.

Práci na vizualizaci provázely problémy s komunikací mezi nainstalovanými servery, což vždy vyřešilo hardwarové restartování budovy. Komunikace byla pravděpodobně narušena nestabilním během programu Iplongate, který byl zahlcen množstvím čtených informací z LonWorks. Aktualizování tohoto programu spolu s pokusem zrychlit komunikační odezvu mezi servery by mohlo být námětem na další práce na budově.

Snímač otisků prstů Moeller M22(S)-ESA byl nainstalován na přední stranu budovy na chodbu. Přístroj MFD-80-(B) byl z důvodu prezentace modelu na výstavách umístěn na venkovní stranu budovy. V praxi bych doporučil tento přístroj umístit dovnitř budovy, neboť snímací jednotka dokáže pracovat samostatně. Důvodem je nutnost zabránit neautorizovanému uživateli, který by se nějakým způsobem dostal ke znalosti bezpečnostního kódu, v pokusu nahrání svého otisku prstu do paměti přístroje a v následném vstoupení do budovy.

Dnešní inteligentní budovy se upínají směrem k používání bezdrátových technologií. Výhodou použití této technologie je snadná montáž, přehledné umístění a případné rychlé přestavění bez potřeby kabeláže. Možností rozšíření modelu budovy v budoucnosti by mohla být aplikace těchto technologií např. použitím kompletního inteligentního systému Xcomfort od společnosti Moeller.

Reference

[dpVV] Vozár, V.: Model automatizace budov, Diplomová práce, Katedra řídicí techniky, ČVUT Praha, 2005

[dpML] Linhart, M.: Komunikační sběrnice LON (LON Operating Network), Diplomová práce, Katedra řídicí techniky, ČVUT Praha, 2004

[Lon] Vojáček, A.: Sběrnice Lonworks, server Automatizace, 2005
1.část URL: http://automatizace.hw.cz/view.php?cisloclanku=2005040501
2.část URL: http://automatizace.hw.cz/view.php?cisloclanku=2005041101
3.část URL: http://automatizace.hw.cz/view.php?cisloclanku=2005061001

[Echelon] Echelon Corporation, 2006 [online]
URL: http://www.echelon.com/solutions/overview/default.htm

[IB] Ing. Schubert, O.: Inteligentní budovy, interakce architektury a technických systémů inteligentních budov, Fakulta architektury ČVUT Praha 2004
URL: http://projekty.fa.cvut.cz/doktorske_studium/2004-prispevky/doktorsky_seminar-2004-o_schubert.pdf

[Sec] Security technologies, moderní zabezpečovací systémy, 2006
URL: http://www.security.cz/cz/produkty/bezpecnostni-systemy.html

[Bio1] plk. JUDr. Vančo, E.: Biometrie, biometrika - geneze, vývoj a současné pojetí, Kriminalistický ústav Praha Policie ČR, Časopis Kriminalistika, č.1/2005
URL: http://www.mvcr.cz/casopisy/kriminalistika/2005/01/vanco_info.html

[Bio2] Bitto, O.: Biometriky nejen v pasech, server Lupa, 2005-09-21,
URL: http://www.lupa.cz/clanky/biometriky-nejen-v-pasech-1/

[Bio3] Fingerprint Analysis [online]
URL: http://en.wikipedia.org/wiki/Fingerprint_analysis

[Moeller] Electronic Security Assembly M22(S)-ESA manual, Moeller, 2006
AWB 1160-1570 GB 5-2005 M22-ESA manual. pdf [online]
URL: http://www.moeller-cz.com/
URL: http://www.moeller-cz.com/pdf/W%201160-7567_0509_M22-ESA%20produktova%20informace_CZ.pdf

[Wiz] Wizcon 9.0 User Guide, Wizcon Systems, 2005 [online]
URL:
http://www.scada.ch/fileadmin/Doku/PR_Wizcon/EN/Axeda%20Supervisor%20Wizcon%209.0%20User%20Guide%20EN.pdf

[ShortStack] ShortStack Developer's Kit product information, Echelon Corp. 2006
URL: http://www.echelon.com/products/development/shortstack/

Přílohy

A. Tabulka Technická data snímače otisků prstů Moeller M22(S)-ESA

Technická data Moeller M22-ESA	
Obecné	
Rozměry zepředu	**(ŠxVxH) 65 x 50 x 16 mm**
Rozměry řídící jednotky	**(ŠxVxH) 76 x 60 x 35 mm**
Instalační hloubka	**45 mm**
Hmotnost	**130g**
Montáž	**2 otvory 22.5 mm**
Okolní podmínky	
Pracovní teplota	**0 – 60 °C**
Skladovací teplota	**-20 – 70 °C**
Relativní vlhkost	**5 – 95%**
Stupeň krytí zepředu	**IP 65**
Stupeň krytí řídící jednotky	**IP 20**
Napájení	
Jmenovité pracovní napětí	**24V DC (+10% - 15%)**
Jmenovitý pracovní proud	**max. 0.2A**
Ztrátový výkon	**5W na 24V**
Releové výstupy	
Počet a typ kontaktu	**1 přepínací kontakt**
Max,.spínací proud	**3 A**
Max. spínací napětí	**15 V - 230 V AC**
Izolační schopnost	
Dimenzování vzdušných a povrchových drah	**EN50178, UL508, CAS22.2 č.142**
Paměť	
Max počet uložených otisků prstů	**100**

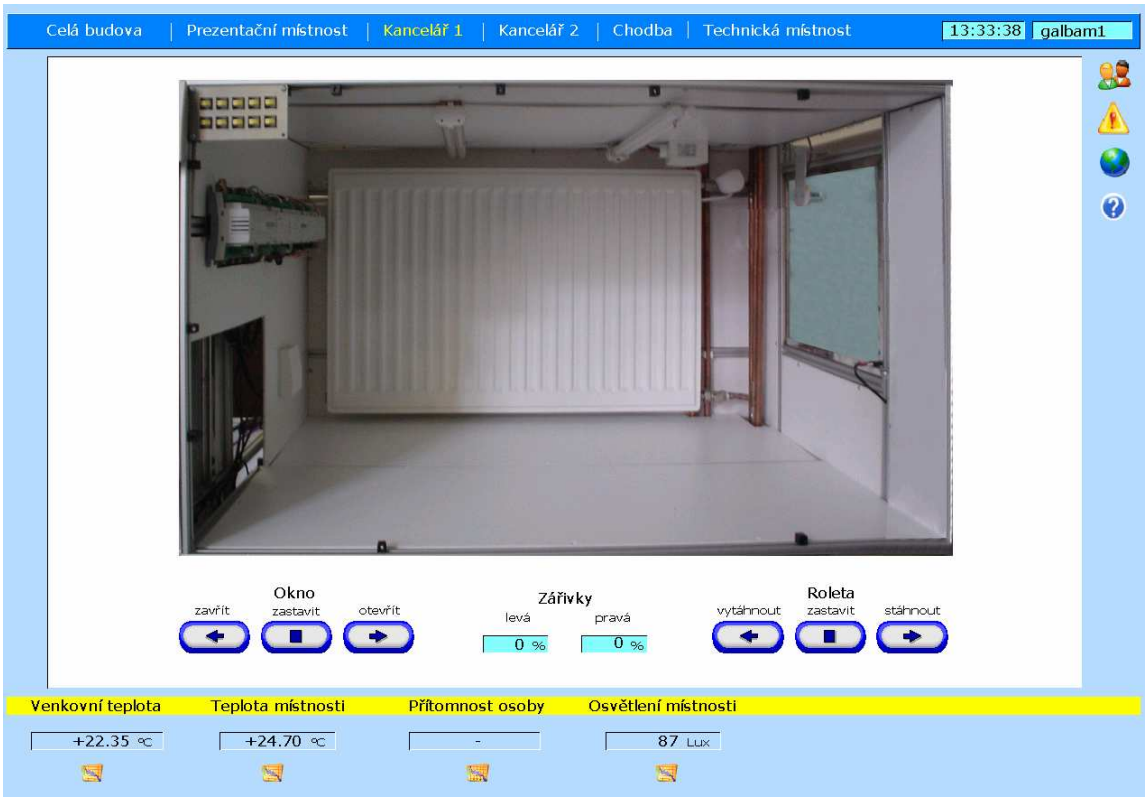
Tabulka A1 - Technická data snímače otisků prstů Moeller M22(S)-ESA

B. Obrázky

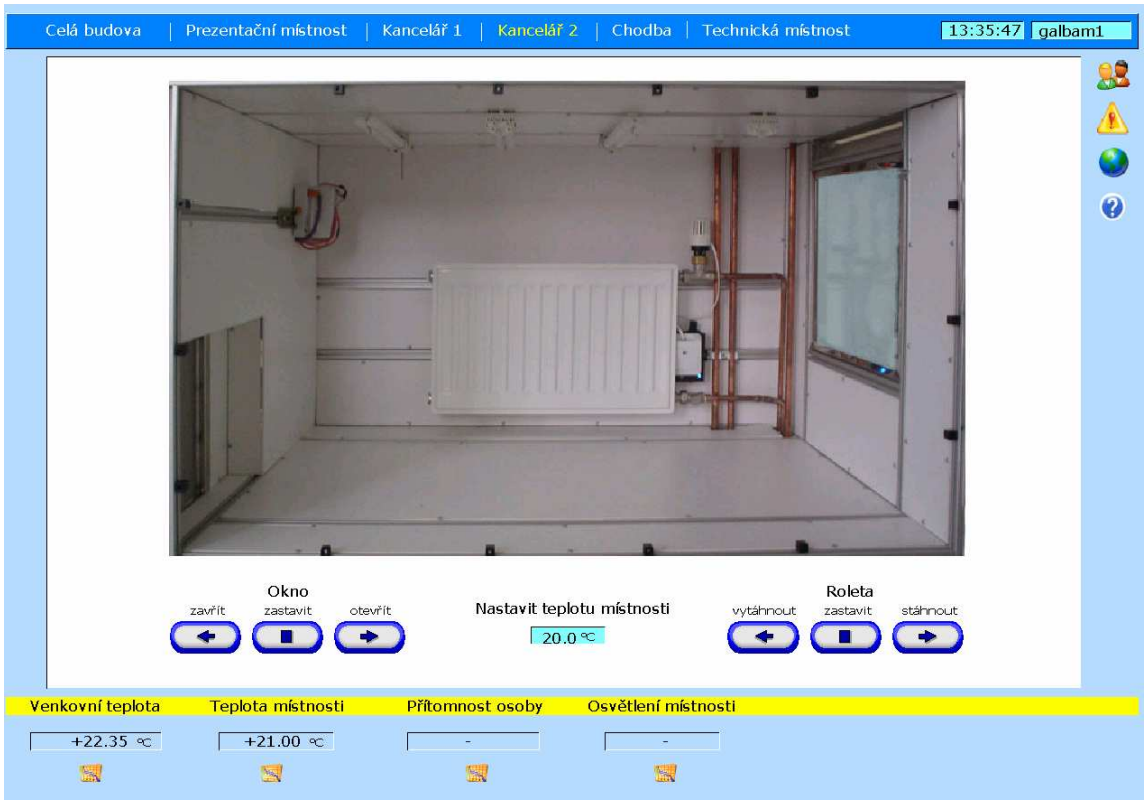
Obrázek B1 - Prezentační místnost v modelu domovní automatizace

Obrázek B2 – Navržená vizualizace - obrazovka "Celá budova"

Obrázek B3 – Navržená vizualizace – obrazovka pro ovládání Prezentační místnosti



Obrázek B4 – Navržená vizualizace - obrazovka pro ovládání Kanceláře č.1



Obrázek B5 – Navržená vizualizace - obrazovka pro ovládání Kanceláře č.2

Obrázek B6 – Navržená vizualizace – předpřipravená obrazovka pro ovládání Výtahu na chodbě

Obrázek B7 – Navržená vizualizace - obrazovka pro ovládání Technické místnosti

C. Obsah přiloženého CD

bp_2006_martin galbavy.pdf	- tato práce ve formátu pdf
bp_2006_martin galbavy.doc	- tato práce ve formátu doc
dokumentace\	- adresář s technickými manuály
software\	- adresář s vytvořenou vizualizací
obrázky\	- adresář s použitými obrázky