DEBRECENI EGYETEM
INFORMATIKAI KAR

Kamerás beléptető rendszer építése a Debreceni Egyetem Műszaki Karának digitális laborjában

Témavezető:
Bartha István Ákos
Tanszéki mérnök

Készítette:
Szabó Sándor
Mérnök-informatikus

Debrecen
2010

Tartalomjegyzék

Plágium – Nyilatkozat

Szakdolgozat készítésére vonatkozó szabályok betartásáról nyilatkozat.
Alulírott (YH974U) jelen nyilatkozat aláírásával kijelentem, hogy a

„Kamerás beléptető rendszer építése a Debreceni Egyetem Műszaki Karának digitális laborjában”

Című szakdolgozat/diplomamunka, (a továbbiakban: dolgozat) önálló munkám, a dolgozat készítése során betartottam a szerzői jogról szóló 1999. évi LXXVI. tv. szabályait, valamint az egyetem által előírt, a dolgozat készítésére vonatkozó szabályokat, különösen a hivatkozások és idézések tekintetében. Kijelentem továbbá, hogy a dolgozat készítése során az önálló munka kitétel tekintetében a konzulenst, illetve a feladatot kiadó oktatót nem tévesztettem meg.

Jelen nyilatkozat aláírásával tudomásul veszem, hogy amennyiben bizonyítható, hogy a dolgozatot nem magam készítettem vagy a dolgozattal kapcsolatban szerzői jogsértés ténye merül fel, a Debreceni Egyetem megtagadja a dolgozat befogadását és ellenem fegyelmi eljárást indíthat.

A dolgozat befogadásának megtagadása és a fegyelmi eljárás indítása nem érinti a szerzői jogsértés miatti egyéb (polgári jogi, szabálysértési jogi, büntetőjogi) jogkövetkezményeket.

Szabó Sándor

Debrecen, 2010.05.12.

1. Bevezetés

Az ipar, a számítástechnika és a korszerű épületek számának növekedésével egyre nagyobb az igény úgynevezett intelligens épületek létrehozására. Elképzelhetetlen manapság egy nagyvállalat, amely olyan nagy értékű eszközökkel dolgozik a vállalat profiljába illő értékteremtő folyamatokon, amelynek ne legyen szüksége a jelenleg a piacon lévő biztonságtechnikai eszközökre. Ezen eszközök vezérlését és felügyelését végzik a különböző épületautomatizálási rendszerek. Napjainkban nem csak nagyvállalatok használják ezeket a rendszereket szinte minden irodaépületet és rengeteg családi házat úgy terveznek meg, hogy annak az épület biztonságtechnika is a része legyen. Az igényeknek az indíttatása minden területen más és más, de egyiknél sem elkerülhető az épületautomatizálás, ami egyben magában foglalja a biztonságtechnikát is. Persze más és más biztonságtechnikai előírások vonatkoznak egy veszélyes anyagokkal foglakozó vállalatra és a dolgozatban létrehozott rendszerre, ami egy műszaki labor felügyeletét végzi, de a lényeg ugyanaz. Értékmegőrzés, felügyelet, nyomon követés. Adott keretek között, és ha megvannak a kellő anyagi források az eszközök megválasztásában, sem lehet nagy különbséget felfedezni, mert felügyelhet ugyanazon rendszer egy vegyi gyárat, és egy családi házat. Lehetőség van rá, de a felhasználók figyelembe véve az igényeiket és a takarékosság szempontjait követve az adott helyet besorolják a biztonságtechnika előírásainak megfelelően, és ez alapján döntenek.

A TAC csoport az épületautomatizálás világpiac egyik meghatározó szereplője. A TAC vállalatcsoport 2003-ban olvadt be a Schneider Electric-be, amely új növekedési perspektívát kínál mindkét fél részére. A TAC az 1925. évi alapítása óta (akkor még Tour Agenturer, 1977-től Tour&Andersson, 1995-től TA Control, majd 1997-től TAC) folyamatosan fejleszti kezdetben gépészeti, ma már teljes épületautomatizálási kínálatát.
Egyik legfontosabb része ennek a teljes körű kínálatnak olyan beléptető rendszerek kialakítása, amely teljes körű felügyeletet ad a belépő és kilépő forgalomról, elkerülve ezzel az illetéktelen behatolásokat.

Dolgozatomban TAC hardverelemek és szoftverek felhasználásával, egy kamerákkal felszerelt mágneskártyás beléptető rendszer kialakítását fogom bemutatni, elemezni, aminek a

végére egy működő a nagyvállalatokéhoz teljes mértékben hasonló rendszer fog létrejönni. Ennek a rendszernek a létrehozását a Debreceni Egyetem Műszaki Karának az első emeletén elhelyezkedő K/7 – s laborban terveztem. Célom egy olyan beléptető rendszer létrehozása, mely a labor biztonságtechnikai követelményeinek maximálisan eleget tesz, és a laborban történő ki-be mozgásokat teljes körűen felügyeli. Felszerelésre kerül még 4 db DSP kamera, amely mozgásérzékelőkkel ellátott, a szerver gép memóriaigényének csökkentése érdekében. Ezen kamerák képeit egy adott gép fogadja és feldolgozza, amelynek segítségével teljes körű lesz a felügyelet a laboron. Épületbitonságtecnikai szempontból a labor nem magas veszélyeztetettségű besorolásba tartozik, de az ittlevő nagy értékű eszközök miatt indokolt egy ilyen rendszer kialakítása. Elméleti jelentősége a dolgozatomnak a rendszertervezésben és létrehozásában van, mert teljes méretekben ilyen megvalósulások működnek manapság vállalati szférában, és a rendelkezésre álló eszközök mind a legjobb minőségűek, a feladat megvalósítására tökéletes célt szolgáltak. Az elkészült rendszernek óriási gyakorlati haszna lesz mindamellett, hogy teljes körű felügyeletet nyújt, de a működő épületfelügyeleti rendszer elkészülésével, prezentálni lehet majd e rendszerek működését, elsajátítani kezelésüket, és konfigurálásuk igény szerint megoldható.

2. Egy általános beléptető rendszer bemutatása

Ebben a fejezetben kifejtem az épület-felügyeleti rendszerek fogalmát, majd ismertetem kialakulásának okait. Továbbá ismertetem az épület-felügyeleti rendszerek csoportosítását, majd kitérek a különböző típusú beléptető rendszerekre, amely ennek a szakdolgozatnak az alapjául szolgáltak. Bemutatom, hogy egy beléptető rendszernek milyen fontos funkciókat kell ellátnia, majd konkrétan kitérek a szakdolgozatban szereplő beléptető rendszerre. [1]

2. 1. *Az épület-felügyeleti rendszer fogalma*

Az épületinformatika az úgynevezett intelligens épületek elektronikai (tűzvédelmi, biztonságtechnikai) és automatizálási (épületgépészet, fűtés, klíma) feladatainak megvalósításával foglalkozó szakterület, melynek hatékony alkalmazásával az épület egyszerűen és gazdaságosan üzemeltethető. Azokat a rendszereket, melyek ezeket a célokat kellő pontossággal megvalósítják és vezérlik, épület-felügyeleti rendszernek nevezzük. [1]

2. 2. *Az épület-felügyeleti rendszerek kialakulásának okai*

Elsődlegesen azokat a főbb okokat kell részletesen megvizsgálnunk amelyek ezen rendszerek széleskörű elterjedését megkövetelték és később az informatika rohamos fejlődésével elősegítették azt.

Hazánkba az 1990-es évek elejétől, közepétől egyre több külföldi befektető érkezett, tette ide székhelyét. Megindult Magyarországra a külföldi tőkebeáramlás, amely elősegítette olyan eddig nem ismert területek fellendülését az iparban, mint az épületautomatizálás. A multinacionális vállalatok szerették volna a pozíciójukat közép-európai szinten is erősíteni, ezért szinte gomba módra elszaporodtak a nagy volumenű beruházások hazánkban is.

Az épületfelügyeleti rendszerek elsődleges felvevőpiacát a külföldi beruházások jelentették. Napjainkra már a régebbi épületek, ipari létesítmények és kisebb hazai beruházások is igénylik a modern, korszerű épület felügyeletet, ezért a külföldi tőke beáramlásával megindult a magyar fellendülés is az épület felügyeleti rendszerek kihasználásában. Automatika rendszerek alkalmazásával lehetővé válik távfelügyelet kialakítása is, ami szintén óriási jelentőségű. Egy olyan cégnél, amelynek több kirendeltsége van országszerte, egy központi helyről felügyelhető az összes helyen történő ki-be mozgás a kamerával szerelt épületfelügyeleti rendszer segítségével. Ezzel a vállalatok csökkentik a munkaerő számát, ami kisebb bérköltség kifizetést eredményezi, ezáltal a rendszer gazdaságossága egyre növekszik. [1]

2. 3. *A szabályozók (DDC-k)*

A számítástechnika egyre nagyobb ütemben terjedő fejlődésének köszönhetően lehetővé vált az épületgépészeti rendszerek hatékonyabb automatizálása, diagnosztikája és regisztrálása. Az egyedileg, szabadon programozható, a személyi számítógépekhez hasonlóan kommunikációs hálózatba köthető mikroszámítógépek, a DDC-k (Direct Digital Control) segítségével lehetőség nyílt a kiterjedt épületgépészeti és épület villamos rendszerek központosított felügyeletére. Ezt nevezzük épület-felügyeleti rendszernek. (Rövidítve: BMS, vagyis Building Management System). [1]

Az épület-felügyeleti rendszerek főbb csoportjai

Az épület-felügyeleti rendszerhez tartozhatnak a következők:

- Villamos energiamenedzsment
- Tűzjelző rendszerek
- **Beléptető és behatolás jelző rendszerek**
- Világítás és redőnyvezérlés
- Zártláncú videó megfigyelő rendszerek (CCTV)
- Épületgépészeti automatika

2. 4. *Egy általános beléptető rendszer működésének leírása*

Napjainkban a beléptető rendszerek feladata, az illetéktelen személyek belépésének megakadályozása a védett területre, a személyforgalom kontrollja, nyilvántartása, a vendégforgalom zavartalan és zökkenőmentes lebonyolítása, ellenőrzése, nyomon követhetősége. A tökéletes beléptető rendszerek stabilak**,** nagy áteresztő képességgel rendelkeznek**,** rugalmasan kezelik a különböző típusú belépőket, és a hozzájuk tartozó jogosultságokat. Ezek a rendszerek hasonlóképpen installálhatók hotelekbe, wellness központokba, iskolákba, cégek számára az igények maximális kiszolgálásával.

Az elektronikus beléptető rendszertől főként azt várjuk el, hogy nappali „nyitott" időszakban mozgó személyek körét ellenőrizze, és a jogosultak körére korlátozza.[2]

Alapvetően a forgalomba helyezett beléptetőknek három fajtáját különböztetjük meg:

- **Online autonóm**

Ebben a működési módban a kontrollerek autonóm egységek, az előre programozott időpontokban képesek a beléptetési pont üzemmódját változtatni. A kontroller saját adatbázisa alapján el tudja dönteni, hogy egy adott időpontban, egy adott kártya áthaladhat-e az ajtón vagy sem. Ismeri az elfogadható kártyák belső kódját és a hozzájuk tartozó időprofilt. Ebben az üzemmódban a rendszer szolgáltat online információkat a Portai és az Épület-felügyeleti kliens szoftver számára. A döntés az ajtó üzemmód és a kártyához tartozó időprofil alapján történik. Az eseményeket a kontroller tárolja, amennyiben a memória tele van, mindig a legrégebbi adatok íródnak felül. Az IP kontroller tárolhat 10. 000 kártyát, 100. 000 eseményt. [2]

- **Anti-passback vezérlős működés**

Az anti-passback ajtónként működik. Anti-passbacknek nevezzük, hogy az a felhasználó nem léphet be, aki a rendszer szerint már bent tartózkodik és fordítva. Ebben a működési módban lehet a rendszer lehetőségeit a legszélesebb körben kiaknázni, mivel a

kontrollerek felett folyamatosan őrködik egy ipari számítógépen futó alközponti szoftver, amely arról dönt, hogy egy adott helyen megjelenő kártya beléphet-e vagy sem. A központi döntés ad lehetőséget komplexebb, a teljes rendszer állapotát figyelembe vevő döntési mechanizmusok definiálására. A több ki- és bejárattal rendelkező helyiségek állapotától függő olyan döntések meghozatalára, amelyek a bent lévő emberek számától vagy személyétől, minősítésétől függenek (pl. nem mehet be dolgozó a pénztárba, ha a pénztáros nincs bent, vagy esetleg ha már egyszerre hárman is bent vannak). A többszintű, hierarchikus anti-passback alkalmazására. A kontrollerek azonnal észreveszik, ha az anti-passback vezérlővel megszakadt a kapcsolat, és automatikusan autonóm működési módba lépnek mindaddig, amíg az anti-passback vezérlő újra meg nem szólítja őket. Ekkor az anti-passback vezérlő egyik első teendője az, hogy a kontrollerekben felgyülemlett eseményeket összegyűjtse és feldolgozza. A feldolgozást követően a kontrollerek újra anti-passback vezérlős működésre váltanak.[2]

- **Offline működés**

A hálózati kapcsolat megszakadása esetén a kontrollerek offline módon működnek. Ebben a működési módban a kontrollerek autonóm egységek, az előre programozott időpontokban képesek a beléptetési pont üzemmódját változtatni. A kontroller saját adatbázisa alapján el tudja dönteni, hogy egy adott időpontban, egy adott kártya áthaladhat-e az ajtón vagy sem. Ismeri az elfogadható kártyák belső kódját és a hozzájuk tartozó időprofilt. Ebben az üzemmódban a rendszer az online információkat nem szolgáltatja, a döntés kizárólag az ajtó üzemmód és a kártyához tartozó időprofil alapján történik. Az eseményeket a kontroller tárolja, amennyiben a memória tele van, mindig a legrégebbi adatok íródnak felül. Az IP kontroller kártyaszámtól függően akár 100. 000 eseményt is tárolhat. Az anti-passback ajtónként működik.[2]

2. 4. 1. *A beléptető rendszer felépítése:*

A rendszer a következő egységekből áll:

- Érintésmentes (proximity) azonosító kártyák
- Kártyaolvasók (5-10-20-30cm-es olvasási távolsággal)
- Forgalomszabályozó eszközök

- Számítógép hálózatba illeszkedő PC rendszerközpont, PC szoftver

Azonosító kártyák:

Az alkalmazott azonosítási technológia nagymértékben befolyásolja egy rendszer rugalmasságát, felhasználóbarát alkalmazhatóságát. A legtöbb esetben egyszerű proximity technológiát alkalmaznak, mely maximálisan megfelel a beléptetés kritériumainak. A kényelmes olvasási távolságok, az azonosítók különböző kivitelei (kártya, kulcstartó), a kártyák azonosító lappal való elláthatósága, az érintésmentes alkalmazás a kártya és az olvasó között biztosítják a felhasználóbarát, egyszerű és gyors használhatóságot. A kártya alkalmas adatok tárolására, segítségével igénybe vehetők egyéb szolgáltatások (pl. öltözőszekrény zárás, iskolai étkeztetés, tankönyvvásárlás, fénymásoló használat, stb.). Természetesen a kártyán kívül további kiviteli formák léteznek, mind például kulcstartó, karóra, stb. A "bankkártya" méretű közelítő (proximity) kártya, hordható levéltárcában vagy kitűzőként egyaránt. A közelítő kártyákra könnyen készíthető színes, grafikus megszemélyesítés.

<u>Előnyei:</u>

- a kártyákat nem kell sehova bedugni, vagy áthúzni (nincs fizikai érintkezés az olvasóval, nincs kopás, elhasználódás)
- egyszerű érintés útján lépnek kontaktusba a forgalomszabályozó, illetve egyéb olvasó berendezésekkel
- a bankkártyákkal együtt hordható a levéltárcában vagy pénztárcában.

A szoftveres megoldások számtalan lehetőséget hordoznak magukban, a megrendelői igények sok esetben eltérőek egymástól. Alapvető elvárás a rendszerrel szemben az, hogy a rendszer kezelje és nyilvántartsa a belépésre jogosultakat, a különböző jogosultsági szinteket, a kezelői jogosultságokat, az időkereteket személyekre és csoportokra bontva, forgóvillákkal felszerelt rendszerek esetén irányfigyelés („be” irányú mozgás után csak „ki” irányú következhet), tartózkodási helyek, törzsadatok, átjáró események, egyéb szűrőfeltételek szerinti lekérdezéseket biztosítson. Igény esetén további szolgáltatásokkal, modulokkal bővíthető a rendszer:

- dolgozók munkaidő nyilvántartása,
- gépjármű beléptetés,
- portai modul: a vendégkártya leadásra egy hangüzenet figyelmeztet, igény esetén vendégkártya elnyelő oszlop illeszthető a rendszerhez,
- véletlenkiválasztó modul (motozás),
- tűzjelző rendszerhez történő illesztés,
- fizetős és egyéb szolgáltatások igénybevételének kezelése, (pl. étterem, fénymásoló stb.),
- öltözőszekrények nyitása, zárása [3]

2. 4. 2. *A beléptető rendszer hardver komponensei*

IP Kontroller (SK03), Buszos IP kontroller (SK03-08), SComplex

A kontroller a beléptető rendszerek egyik alapeszköze. A kontroller két fő részből áll: a központi modulból, valamint a periféria modulból. A központi modullal lehet a strukturált hálózatra csatlakoztatni. A központi modul fogadja a kártyaolvasó jeleit, tárolja mindazt az információt, mely a beléptetéshez szükséges, nyitja az ajtót és naplózza az eseményeket. A központi modul a tárolt jogosultság és időadatok alapján aktiválja az elektromos zárat. A periféria modulon vannak a relék és a sorkapcsok. A kontroller két olvasót tud kezelni. A két olvasót az ajtó két oldalára szerelve a kontroller meg tudja különböztetni a ki- és belépést.

IP kontroller (SK03)

Egy belépési pont ki- és be irányú proximity olvasóit tudja kezelni. Vezérelni tud két sorompót, forgóvillát, ajtózárat. Csatlakoztatható hozzá kettő pin kód vagy munkaidő terminál, ajtónyitó gomb. Tárolhat 10. 000 felhasználói adatot, 100. 000 eseményt. A tűzjelzővel összekötve tűzjelzésre kinyitja az ajtót.

Buszos IP kontroller (SK03-08)

Több belépési pont 8 kártyaolvasóját tudja kezelni ki- és be irányban. Csatlakoztatható hozzá buszos pin kód, ajtónyitó gomb. Az ajtónyitáshoz szükséges relét a kártyaolvasó tartalmazza. Két olvasó közötti távolság 1 km lehet.

SComplex központ (SC01)

Egy belépési pont ki- és be irányú proximity olvasóit tudja kezelni. Vezérelni tud két sorompót, forgóvillát. Csatlakoztatható hozzá kettő pin kód vagy munkaidő terminál, ajtónyitó gomb. Tárolhat 10. 000 felhasználói adatot, 100. 000 eseményt. A tűzjelzővel összekötve tűzjelzésre kinyitja az ajtót.

Proximity kártyaolvasó

A kontrollerhez proximity kártya olvasására alkalmas olvasó berendezést kell telepíteni. Beléptető rendszerekhez proximity szabvány MIFARE proximity kártyákat, kezelő olvasót installálnak. Az olvasó a felhasználónak hang és fényjelzéssel jelzi, ha a rendszer elolvasta a kártyáját, és ha esetleg őt valamilyen okból nem engedte be. Az olvasó és a kontroller távolsága több tíz méter is lehet, ezért a kontroller kényelmesen telepíthető.[4]

2. 4. 3. *A beléptető rendszer szoftver komponensei*

Beléptető szerver

Ez a program egy SQL adatbázis kezelőre épített applikációs szerver program. A szerver folyamatosan megkapja az alközpontról a naplóadatokat, feldolgozza azokat, és 1500 bites RSA titkosítással védett virtuális csatornán keresztül SQL alapú hozzáférést biztosít ezekhez, az adatokhoz a kliens programok számára.

Konfiguráló kliens program

Ezzel a programmal lehet a rendszert konfigurálni, a felhasználók jogosultságait változtatni. Megszemélyesítés után a kártyák adatbázisba való felvitelét egyszerűsíti a számítógéphez csatlakoztatott soros olvasó. Ha megváltoztatjuk a rendszer konfigurációját, akkor ezt le kell tölteni az ajtóvezérlőkbe.

Napló megjelenítő kliens program

Ezzel a programmal lehet a bekövetkezett eseményeket utólagosan nyomon követni. A program a naplózott eseményeket különböző szempontok szerint csoportosíthatja és jelenítheti meg.

Épület-felügyeleti kliens, riasztás megjelenítő modul

Ez a program az őröknél elhelyezett számítógépen fut és jelzi, hogy riasztás történt. Az őrök a számítógéppel tudják nyugtázni a riasztásokat. Az őrök beavatkozását a rendszer naplózza.

Vendégkártya kiadó kliens program

Ez a program képes a vendégek számára kiadott kártyákhoz belépési jogosultságot rendelni. A vendégek adatait elektronikus formában rögzíti. A vendégkártya kiadását gyorsítja, hogy a program megjegyzi a vendégek adatait, így néhány karakter leütésével megtalálható egy korábbi látogatás során bevitt adat.

Munkaidő nyilvántartó program

A beléptető rendszerek egy privát nagyon speciális csoportját képezik a munkaidő nyilvántartóval felruházott megvalósulások, amelyek számos a már tárgyalt funkciókon kívüli tulajdonsággal látja el az épületinformatikai rendszereinket. A munkaidő nyilvántartó program egy speciális kliensprogram. Ez a program a munkaidő nyilvántartási törzsadatok, és a naplózott események alapján elkészíti azokat a nyomtatott és elektronikus listákat, melyek a bérszámfejtés alapját képezhetik.

A munkaidő nyilvántartóval felszerelt beléptető rendszer szolgáltatásai a következők:

- **Gyors és megbízható azonosítás:** Proximity kártyával gyorsan és kényelmesen azonosíthatók a dolgozók, a bejáratok nagyobb terhelést

tudnak elviselni. Kevesebb belépő kapu kialakítására van szükség, ami csökkenti a munkaidő nyilvántartó rendszer kiépítésének költségeit.

- **Rugalmas jogcím kezelés:** A rendszer akár 255 ki és belépési jogcímet is le tud a kezelni, mellyel a felhasználói igények maradéktalanul kielégíthetők.
- **Balanszidő kijelzés:** Rugalmas munkarendben dolgozók folyamatosan nyomon követhetik a munkaidő egyenlegüket a munkaidő nyilvántartó terminál kijelzőjén.
- **Azonnali adatszolgáltatás:** A dolgozókra vonatkozó információk tetszőleges időpontban lekérdezhetők.
- **Felülbírálhatóság:** A dolgozó munkaidejére vonatkozó adatokat (hiányzás, túlóra, stb.) a közvetlen munkahelyi vezetők felül tudják bírálni.
- **Kapcsolódási lehetőség a bérszámfejtő rendszerhez:** A program képes előállítani olyan adatbázist, mely a bérszámfejtő rendszer által közvetlenül feldolgozható.
- **Kapcsolódási lehetőség a vállalatirányítási rendszerhez (SAP, Oracle):** A vállalatirányítási rendszerből a törzsadatokat automatikusan lehet a munkaidő nyilvántartó rendszerbe importálni.

Számos esetben az alapprogramhoz bővítő modulokként, az igények átgondolásával vásárolhatjuk meg az előbbiekben bemutatott szolgáltatásokat. A vezérlő számítógépen futtatni kívánt beléptető rendszert vezérlő szoftvert számos az alapfunkciókon túl bemutatott tulajdonságokkal bír, ezek viszont költségesebbek nemcsak a szerelés terén, de karbantartásukkal is egyenesen arányos módon, fokozottan kell eljárni.[4]

3. TAC beléptető rendszer létrehozásához választható eszközök:

Ebben a részben ismertetem a TAC nagyvállalat által kínált biztonságtechnikai rendszert és a működéséhez szükséges lehetséges eszközeit.

TAC a nyílt, integrált épületinformatikai rendszerek piacvezető gyártója.
A TAC küldetése világszerte az, hogy minél több hozzáadott értéket nyújtson a végfelhasználók és az épülettulajdonosok számára az épületgépészeti és biztonságtechnikai rendszerein keresztül. A TAC több mint 80 éves épületgépészeti, - automatizálási és biztonságtechnikai tapasztalattal, 5000 alkalmazottal, partnerhálózattal és leányvállalatokkal a világ 80 országában van jelen.
TAC anyavállalata a Schneider Electric, az automatizálás és energiaelosztás piacvezető résztvevője, mely a világ 130 országában 105 000 alkalmazottal rendelkezik. TAC a leggyorsabban fejlődő és az egyik leginnovatívabb résztvevője az épületautomatizálási iparágnak: évről évre és épületről épületre a megrendelők elvárásaik maximális kielégítésével készítik épületinformatikai rendszereiket.[5]

1. ábra: Az Andover Continum Infinet vezérlő család

Az Andover Continuum vezérlők, felhasználói interfészek és szoftvereszközök teljes rendszere, melyek többféleképpen kombinálhatók a mindenkori felhasználói igényeknek megfelelően. Legyen szó egyetlen főiskolai laborról vagy több telephelyes épületről, az Andover Continuum könnyen alkalmazható és bővíthető. Speciális területek igényeire is testre szabható. A szigorúan ellenőrzött élettudományi területen is telepíthető és validálható a rendszer úgy, hogy megfeleljen az FDA szabályozásainak. Az Andover Continuum Ethernet

alapú hálózati vezérlői az iparág legerőteljesebb vezérlői, melyek messze meghaladják az alap útválasztási funkciókat. Programozható vezérlőként, web szerverként, protokollillesztőként, valamint riasztás- és eseménytovábbító eszközként egyaránt működhetnek. A létesítmények működése nagyban függ a vezérlőrendszer megbízhatóságától. Éppen ezért osztotta le a TAC az intelligenciát a terepi vezérlők szintjére. Ezek a vezérlők önálló működést és vezérlést biztosítanak, futtatják saját programjaikat, időprogramjaikat, trendjeiket, elküldik a saját riasztásaikat és eseményeiket. Az Andover Continuum rendszerhez csatlakoztatva a terepi adatbuszt, a vezérlők globálisan meg tudják osztani egymás között az adataikat. Ez a globális adatpont címzés lehetővé teszi a magas szintű koordinált vezérlést és a költségek csökkentését.

2. ábra: Continum bCX1 hálózati vezérlő

A Continuum bCX1 egy gazdag szolgáltatáskészlettel bíró, költséghatékony hálózati vezérlő, mely támogatja az Infinity terepi vezérlőcsaládot. A vezérlő 10/100 Ethernet hálózati kártyával rendelkezik, maximum 127 db Infinity vezérlővel képes kommunikálni, a 2. kommunikációs portjához modem csatlakoztatható, illetve Plain English meghajtóprogrammal is használható. A hálózati vezérlő hozzáférést biztosít a hozzá csatlakozó terepi vezérlőkhöz és egy egyszerű, könnyen használható konfigurációs interfészen keresztül konfigurálható. A bCX1 TCP/IP interfészén keresztül hozzáférhetőek a benne létrehozható egyedi felhasználói weblapok, emellett SNMP felügyeletre és riasztás küldésre is lehetőséget biztosít. A bCX1 vezérlőhöz az xP bővítő modulok részére bővítő porttal is rendelkezik, mellyel helyi I/O vezérlések is elvégezhetőek.

- 10/100 Ethernet port
- helyi I/O modulokkal és kijelzővel bővíthető (Andover xP modulok)
- fejlett Flash memória nagyfokú megbízhatóságot nyújt – Ebben tárolja az alkalmazás programokat, operációs rendszert, működési adatokat
- a Flash memória lehetővé teszi az online frissítéseket
- telefonos betárcsázási funkció
- egyedi weblapkészítés lehetséges
- SNMP felügyelet
- SNMP riasztás opció lehetséges
- XDriver opció lehetséges
- redundáns riasztási támogatás

Műszaki jellemzők

Tápellátás: 24 VAC, +10% -15%, 50/60 Hz, 12-28 VDC auto felismerés

Működési tartomány: 0–+49°C 10–95% RH (nem kondenzálódó)

Méretek (magasság x szélesség x mélység): 139 mm x 213 mm x 62 mm

Akkumulátor: Cserélhető, tölthető akkumulátor. Jellemzően 30 napig képes megőrizni a RAM-ban tárolt adatokat. Az összes adatot Flash-ben tárolja áramkimaradás esetén.

Memória: 32 MB SDRAM, 16 MB FLASH. [5]

XDriver támogatás

Használhatjuk a bCX1-et hatékony átjáróként más gyártók rendszereihez azáltal, hogy XDriver opciót rendelünk a vezérlő valamelyik komm portjához. Az XDriver használatával az Andover Continuum rendszerébe integrálhatóak más gyártók rendszerei, lehetővé téve ez által az egész rendszer programozhatóságát Plain English-ben, valamint felügyeletét és megjelenítését, a CyberStation munkaállomásán vagy a web.Client felületén keresztül.

3. ábra: NetContoller

A TAC nagy teljesítményű hálózati menedzsmentet biztosít a Continuum CX vezérlőcsaládjával.

A NetControllerek LON technológiára épülő I/O modulokat használnak. A Continuum Infinet terepi vezérlők önálló DDC vezérlést biztosítanak az épülethez. A Continuum hálózati vezérlők rendszerkoordinátorként működnek az intelligens elosztott I/O modulokhoz, biztosítva ezzel:

- a hálózati kommunikációt és az integrált globális vezérlést az Ethernet hálózaton keresztül,
- a teljes programozhatóságot a Plain English programozási nyelv használatával,
- a felhaszálóbarát menüvezérelt interfészt,
- a helyi és távoli riasztást,
- a TCP/IP (internet) protokoll használatát,
- a programozható RS-232/485 portokat modemekhez, terminálokhoz és nyomtatókhoz,
- a közvetlen programozható soros kommunikációt más gyártó eszközeivel,
- az opcionális parancssor interfészt,
- a csatlakozást 2 db RS-485 alapú Infinet terepi adatbuszhoz,
- a beépített webszervert,
- a Netcontroller I és Netcontroller II használhatóságát. [5]

Continuum CX9900 tápegység (PSU)

A Continuum CX9900 tápegység 24 VDC tápellátást biztosít a CX9900 NetController (vagy

NetController II) és a kapcsolódó I/O modulok számára. Megtáplálható 120-240 VACval és opcionálisan teljes UPS képesség is rendelhető hozzá. Az akkumulátoros üzemmód kiválasztásának lehetősége Plain English programozási nyelven keresztül lehetséges.
Az egységalapra és DIN-sínre is szerelhető, gyorscsatlakozókkal rendelkezik a NetControllerhez és az I/O modulokhoz. CE megfelelősség.

4. ábra: NetController II CPU modul

NetController II CPU modul

Az Andover Continuum NetController II a NetController első sorozatának újratervezett változata, ez a készülék a nagy teljesítményű központi vezérlőegység (CPU) modulja és hálózati menedzsere az Andover Continuum intelligens épületautomatika rendszerének. 128 MB DDR SDRAM-mal, 32 MB Flash-sel és 4 programozható kommunikációs portjával (beleértve az Infinity portot) a NetController II teljes megoldást biztosít a létesítmény egészére – a hálózati kommunikációra és az információkezelésre – vonatkozóan. A teljes DDR memóriakapacitásból 12 MB az alkalmazások és a működési adatok számára, 48 MB a személyi adatok tárolására van fenntartva.
A NetController II Continuum CyberStation szoftver 1.8 verziójától alkalmazható, és olyan új szolgáltatásokat tartalmaz, mint a hálózati biztonság, területi lezárás és e-mail küldés.

- ethernet IP-alapú hálózati vezérlő
- hatékony, moduláris CPU-kártya az Andover Continuum I/O modulok és Infinet vezérlők vezérlésére és felügyeletére
- nagy sebességű hálózat – 4 millió eszköz az Etherneten
- négy programozható komm. port a rugalmas integrációhoz
- a programozható akkumulátor tartalék, lehetőséget ad a lekapcsolási üzemmód megválasztására

- flash, könnyű online szoftverfrissítésekhez
- andover Plain English leegyszerűsíti a programozást
- DIN-sínre szerelhető, egymásba csúszó csatlakozók
- lefelé kompatibilis
- biztonságos Ethernet kommunikáció IPsec/IKE titkosítás és hardveres gyorsítás
- könnyű konfigurálhatóság a beépített weblapok segítségével
- területi lezárás, illetve fenyegetettségi szint-alapú hozzáférési jogok
- 32 db vezeték nélküli Infinet vezérlő csatlakoztatható hozzá

Műszaki jellemzők

Tápellátás: 24 VAC, 50/60 Hz, 12-28 VDC autó-felismerés

Működési tartomány: 0°C–+49°C, 10-95% RH (nem kondenzálódó)

Méretek (magasság x szélesség x mélység): 222, 3 mm x 152, 4 mm x 63, 5 mm

Akkumulátor: Tölthető akkumulátorok, 60 perc szünetmentes üzemidő, 35 Watt fogyasztás esetén; 7 napig védi a DDR SDRAM és a rendszerórát, bővíthető I/O busz: 32 db I/O modul közvetlenül csatlakoztatható. [5]

5. ábra: Continuum CX9900 központi vezérlőegység (CPU)

Continuum CX9900 központi vezérlőegység (CPU)

A Continuum CX9900 CPU Continuum I/O modulokhoz és az Infinet vezérlőkhöz biztosít felügyeletet és vezérlést. A Flash memória lehetővé teszi a könnyű online frissítést a szabadon programozható Plain English programnyelven. A CX9900 összekapcsolja a nagy sebességű Ethernet és a helyi terepi hálózatokat. Sínre szerelhető kivitelben készül.

- ACC-LON RS-485 és ACC-LON FTT-10A protokoll opciók
- csavart érpár (10 Base T) vagy üvegszálas optika (10 Base F) opciók
- programozható RS-232/485 portok (4) modemekhez, terminálokhoz és nyomtatókhoz
- LED-es állapotkijelzés
- fogyasztás 10 Watt, 24 VDC max
- a 8 MB RAM-mal rendelkező NetController matematikai társprocesszort tartalmaz
- webszerver alapszolgáltatás
- biztonságtechnikai rendszereknél:

4 MB RAM modulok – 5000 személyi rekord

8 MB RAM modulok – 78000 személyi rekord

6. ábra: ACX vezérlő

ACX sorozat Ethernetre

Az ethernetes ACX vezérlők az Andover Continuum termékcsalád legerőteljesebb beléptetés vezérlői. A kezdetektől arra tervezték, hogy az USA kormánya által kidolgozott biztonságtechnikai előírásoknak megfeleljen.

Beépített I/O csatornák a beléptetés vezérléshez

Két alap hardver modell rendelhető: 5720 és 5740. Az 5740 jelzésű modell dupla I/O kapacitással rendelkezik az 5720-hoz képest. Az ACX-eket arra tervezték, hogy a kilépő és belépő oldali olvasókat is támogassák, melyeknek +5 vagy +12 VDC tápfeszültséget tudnak biztosítani (120 mA és 180 mA).

- 10/100 Base-T Ethernet, 192-bit IPsec/IKE titkosítás – gyors és biztonságos IP kommunikáció biztonságtechnikához
- 480 ezer személyi rekord tárolható
- 32 MB Flash memória és 128 MB dinamikus RAM biztosítja a dinamikus memória hozzáférést
- magas szintű kártyaolvasó bemenetek dedikált processzorral – a legújabb olvasó megoldások támogatása
- támogatja a területlezárási funkciót
- „fenyegetettségi szint” függő belépési jogok támogatása
- xP modulokkal bővíthető – a vezérlő így az egyedi igényekre szabható
- teljes körű kártya formátum támogatás 256 bitig – támogatja a múltat, miközben a beléptető rendszerek jövőjére tervez
- SNMP támogatás –a beléptető rendszer egyszerű, IT-barát megfigyelését biztosítja
- Modbus XDriver támogatás – lehetővé teszi Modbus-os eszköz hozzákapcsolását a rendszerhez [5]

7. ábra: CX9702 beléptetésvezérlő

CX9702 beléptetésvezérlő

Kisméretű, személyzet nélküli vagy távoli helyszíneken való alkalmazásokhoz tervezték.

A CX9702 beléptetés vezérlő hálózatos elektronikus beléptetés vezérlésre, hőmérsékletszabályozásra, riasztás monitorozásra alkalmas, egyszerű és költség hatékony vezérlő. Önálló működésre alkalmas eszköz, mely 2 ajtót képes vezérelni. 4 felügyelt bemenettel, 4 univerzális bemenettel és 2 digitális kimenettel rendelkezik épületgépészeti berendezések vezérléséhez.

A ráépített Infinet buszon keresztül a rendszer bővíthető további 4 db Infinet vezérlővel.

A CX9702 része lehet az integrált Continuum létesítménymenedzsment rendszernek, és felügyelhető, illetve irányítható a Continuum CyberStation felügyeleti munkaállomáson vagy a web.Clienten keresztül. A dinamikus grafikus képernyőkön keresztül a felhasználó riasztásokat kezelhet, megjelenítheti az élő paramétereket és módosíthatja az alapjeleket.

A biztonságtechnikai beállítások módosíthatóak, hozzáférések adhatók, illetve visszavonhatók.

A digitális videó rendszerhez kapcsolódva az eszközben észlelt riasztás felugró kameraképet eredményezhet a munkaállomás képernyőjén.

- egyszerű, gazdaságos megoldás kis, kezelő néküli vagy távoli telekom alkalmazásokhoz:
- riasztás felügyelet
- beléptetés vezérlés
- hőmérséklet-szabályozás
- TCP/IP kommunikáció az Ethernet hálózatba szervezéshez
- hőmérséklet, páratartalom, tűzjelzés és energiafelhasználás monitorozása az univerzális bemenetekkel

- SNMP kompatibilis – Riasztások kezelését teszi lehetővé a más gyártók hálózati rendszereivel
- támogatja a web.Client felhasználói felületet
- Continuum Infinet vezérlőkkel bővíthető
- normál és szünetmentes tápellátás biztosítása a zárakhoz, olvasókhoz, perifériákhoz
- össz. adatpontszám: 8 bemenet, 2 kártyaolvasó bemenet, 4 kimenet. [5]

8. ábra: i2 xP I/O bővítőmodulok

i2 xP I/O bővítő modulok

Az Infinet II (i2) „plug-in" bővítőmoduljai segítségével könnyen, rugalmasan és költség hatékonyan adhatunk további I/O kapacitást a vezérlőkhöz. Maximum 2 modul és 1, legfeljebb 3 méterre elhelyezhető kijelző csatlakoztatható a vezérlőkhöz. Maximum 180 mA áll rendelkezésre a bővítő modulok számára az Infinity vezérlőkben. Külső tápegységgel sem adhatóak további modulok egy vezérlőhöz.

- Csak az alábbi vezérlők alkalmasak i2 xP modulok fogadására:
  i2920, i2810, i2814, i2850, i2851, i2853, bCX1 CR és ACX
- IP20 védelem
- CE megfelelőség

Andover Continuum BACnet vezérlőcsalád

9. ábra: Andover Continuum BACnet vezérlőcsalád

BACnet együttműködés, minden szinten:

A nyílt szabványok a szabad választás lehetőségét biztosítják az épülettulajdonosoknak az épületautomatika rendszerekre vonatkozólag. A BACnet nyílt szabvány egy olyan univerzális modellt biztosít az épületautomatika rendszerek készítéséhez, mely alapján az elkészült rendszer más rendszerekkel is képes együttműködni. Az Andover Continuum rendszer kihasználja a BACnet adatmegosztási, naplózási, ütemezési, riasztási, és eszközmenedzsment funkciók előnyeit. A BACnet operátori munkaállomástól kezdve, a nagy épületvezérlőkön át a legkisebb terepi vezérlőig az Andover BACnet termékcsaládja a legmagasabb szintű együttműködést biztosítja, minden szinten. [5]

Andover Continuum mint BACnet rendszer:

A BACnet összes előnyének kihasználásához fontos, hogy az egész rendszer eredendően BACnet kompatibilis legyen. Az Andover Continuum a BACnetet használja a kommunikációhoz a rendszer minden szintjén. Az Andover Continuum rendszer rendelkezik BACnet operátori munkaállomással (B-OWS) és BACnet épületvezérlőkkel (B-BC), melyeket rendszermenedzsmenthez és a BACnet üzenetek továbbítására használ; de ezek az eszközök csak egy részét képezik a Andover Continuum BACnet megoldásnak. Nagyon fontos, hogy a BACnet kompatibilitás a teljes BACnet MS/TP vezérlőcsaládra igaz legyen, melyek tárolják és futtatják saját programjaikat, a BACnet trendeket, BACnet időprogramokat és BACnet riasztásokat, ezáltal növelve a teljesítményt és a megbízhatóságot. Ezen túl az együttműködési képesség is nő, miközben csökkennek a telepítési költségek. Például ugyanaz a BACnet MS/TP hálózat, amelyet a Andover Continuum BACnet terepi vezérlők

használnak, alkalmas olyan más gyártótól származó biztonságtechnikei rendszer kezelésére, amely tartalmaz BACnet vezérlő.

Továbbá, a nyílt architektúrának köszönhetően az Andover Continuum lehetővé teszi az Andover Continuum beléptetés vezérlői, világításvezérlői, digitális videó rögzítői és több mint 200 protokollja számára az együttműködést a natív, TAC-tól és más gyártótól származó BACnet eszközökkel. [5]

10. ábra: Vezérlő/router sorozat bCX1

Az *Andover Continuum bCX1* sorozatú vezérlői, BACnet kompatibilis routerek és vezérlő/ routerek. Ezek a vezérlők a hálózati szinten működnek és a BACnet üzeneteket továbbítják a BACnet/IP, BACnet over Ethernet és MS/TP hálózatok között. BBMD-ként is működhetnek (BACnet Broadcast Management Devices), lehetővé téve az üzenetek továbbítását IP hálózatok között.

Két alapmodell készül: a bCX1-R (csak router) és a bCX1-CR (vezérlő/router). A bCX1-R modell teljes funkciós BACnet router BACnet hálózatok között, a bCX1-CR, pedig egy teljes funkciós épületvezérlő is egyben (B-BC). A bCX1-CR ugyanúgy viselkedik routerként, mint a bCX1-R, kiegészítve a programozható I/O kezelési tulajdonsággal.

- B-BC - BACnet épületvezérlő elérhető router és vezérlő/router verzióban is
- 18 BACnet objektumtípust támogat, pl.: trendek, időprogramok, naptárak és hurkok
- igazi BACnet/IP és MS/TP kommunikáció a más gyártó eszközével való együttműködés érdekében
- 10/100 Ethernet port
- BACnet Broadcast Message Device (BBMD) támogatás
- bővíthető lokális I/O-val és kijelzővel az xP bővítőcsaládból

• fejlett Flash memória nagyfokú megbízhatóságot nyújt – Ebben tárolja az alkalmazásprogramokat, az operációs rendszert és működési adatokat

• a Flash memória lehetővé teszi az online frissítéseket

• egyedi weblapkészítés lehetséges

• BTL tesztelt B-AAC vezérlő lokális trend funkcióval

Műszaki jellemzők

Tápellátás: 24 VAC, +10% -15%, 50/60 Hz, 12-28 VDC auto felismerés

Működési tartomány: 0–+49°C 10–95% RH (nem kondenzálódó)

Méretek (magasság x szélesség x mélység): 139 mm x 213 mm x 62 mm

Akkumulátor: Cserélhető, tölthető akkumulátor. Jellemzően 30 napig képes megőrizni a RAM-ban tárolt adatokat. Az összes adatot Flash-ben tárolja áramkimaradás esetén.

Memória: 32 MB SDRAM, 16 MB Flash. [5]

4. Egyéb eszközök

4. 1. CNB típusú színes kamerák

11. ábra: CNB kamera

A CNB kamera általános jellemzői:

- 1/3” Super HAD CCD, DSP
- felbontás: 520TV sor
- fényérzékenység: színes (0.3lus), FF (0.1lux)
- OSD menü
- AGC, BLC, remegésmentesség
- beépített mozgásérzékelés (64db zóna)
- privát zóna kitakarás (4db)
- tükör funkció
- tápellátás: 12V DC, max. 140mA

[6]

4. 2. Azonosító kártyák

12. ábra: INDALA azonosító kártya

Az INDALA közelítő kártyák olvasási távolsága rendkívül következetes. A különböző környezeti feltételek, vagy az emberi testárnyékoló hatása nem befolyásolja a működését, így például kulcsok vagy pénzérmék közelsége sem. Vékony, a bankkártyákkal együtt hordható a levéltárcában vagy pénztárcában.

Hosszú élettartam: az image 30 ISO közelítő kártya elem nélkül működik, ezáltal számtalan olvasás tesz lehetővé.

Tartósság: az Image 30 ISO közelítő kártyák flexibilis anyagból (PVC) készültek, így a törés szempontjából ellenállóak.

Felhasználói grafikák: felhasználó specifikus színes grafikák készíthetőek rá. [7]

4. 3. Beléptető modulok

13. ábra: INDALA olvasó

INDALA Olvasók: a SEAWING rendszerbe integrálható közelítő kártyás olvasók kielégítik mindazon igényeket, melyeket napjaink biztonságtechnikája megkövetel. Az olvasócsalád tagjai kompakt eszközök, melyek lehetővé teszik Motorola-Indala típusú kártyák felismerését. Az olvasó által szolgáltatott adatok (kártya információk, PIN kódok) rendszerszinten feldolgozhatók (pl. beléptető terminál segítségével).

Elsődleges jellemzőik:

- Műanyag burkolat
- Beltéri/kültéri kivitel
- Hangjelzés és LED - es állapot kijelzés

Működési elv:
Az olvasó 125kHz-es frekvenciájú szinuszos jelet sugároz ki, amely az olvasási távolságon belül elegendő energiát szolgáltat az azonosító kártyának ahhoz, hogy visszasugározza 62,5 kHz-en az egyedi kódját, amit az olvasó felismer, és átalakítás után továbbít. [8]

4. 4. Kis automaták a rendszerben

14. ábra: C60N kis automata

Funkció:

A kismegszakítók a következő funkciókat egyesítik:

- áramkörök védelme a rövidzárlati áramok ellen
- áramkörök védelme a túlterhelés ellen
- vezérlés
- leválasztás
- személyek védelme közvetett érintés ellen, TN és IT rendszerben
- a C60N kismegszakító szolgáltatási és ipari környezetben egyaránt használható

Jellemzők:

Teljesítménykör:

- üzemi feszültség: 440 V

- megszakító képesség: MSZ EN 60-947-2 szerint Icu végleges zárlati határmegszakító képesség (O-CO ciklus) [9]

5. Eszközválasztás

Ebben a részben összefoglalom a diplomamunkámban szereplő beléptető rendszerhez ár-érték arányban kiválasztott eszközöket automatizálási és terepi szinten.

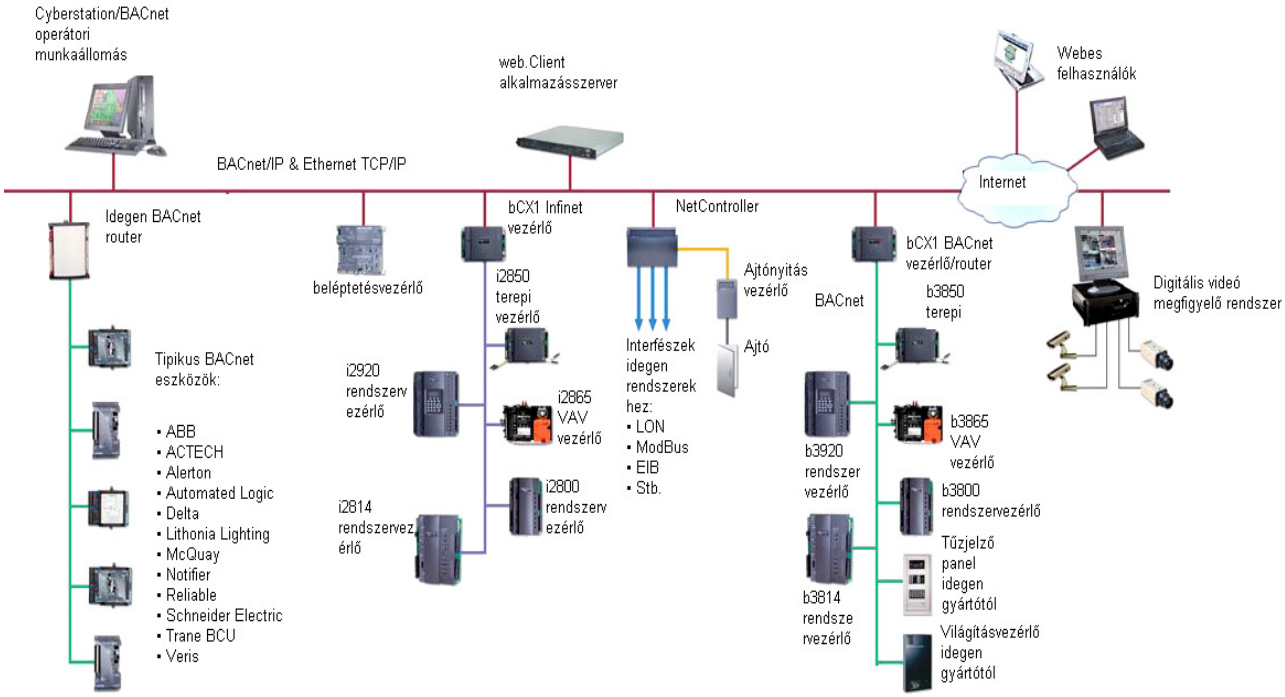
A rendszer tartalmaz egy andover continuum Acx 5740 es beléptetési vezérlőt, amely rendelkezik integrált I/O csatornákkal. A laborban a faliszekrénybe lettek beépítve a c60n automaták, melyek védik a rendszert a rövidzárlati és a rendszer túlterhelése következtében fellépő áramok ellen. A felszerelésre került négy analóg kamera a faliszekrényben lévő vezérlővel utp kábel összeköttetéssel kommunikál. A szabvány analóg videó jeleket ezek a kábelek továbbítják majd a vezérlő, beépített digitalizáló kártyájának segítségével a beérkező analóg jelet digitalizálja, majd tömöríti. A felszerelésre került 4 kamera mozgásérzékelős funkciókkal bír, így csak akkor indítja el a rögzítést, amelyik időpillanatban mozgást érzékel a laborban. A rögzített videók szabványos mpeg 4 formátumban kerülnek tárolásra a szerver gépen, amely tetszőlegesen bővíthető szabványos HDD- kel. A szervergép memóriájának elfogyásával a rendszerünk a fifo elv alapján a legrégebben tárolt adatokat üríti és helyükre az új, aktuálisan felvett videók kerülnek.

Kamera minőségét behatárolja a használt video szabvány. Esetünkben Pal szabványt használva a felbontás 625 soros, ebből 575 sor a látható kép. 50 Hz képfrissítés, ami a váltott soros megjelenítés miatt 25 egészképet jelent. A tömörítés minőségét, és sebességét (f/s) a használt rögzítő kártya határozza meg. Eszközeink váltott soros megjelenítéssel működnek. 50 félkép másodpercenként. Először a páratlan sorok, majd a páros sorok kerülnek továbbításra. Emiatt a gyorsan mozgó objektumok képe sok esetben fésűszerűen szétcsúszik a képeken. Minél kisebb f/s érték jut egy kamerára, annál nagyobb az időbeli eltérés a két fél kép kocka között, ezzel arányban nő a szétcsúszás is. Analóg videojeleket maximum 300m-ig lehet átvinni még a legjobb minőségű csatlakozók és kábelek használata mellett is. Esetünkben a kamerák és a vezérlők között nagyságrenddel kisebb a távolság ezért ideális megvalósulásnak bizonyult ez a kialakítás.

A beléptető rendszer terepi szintjén elhelyezkedő beléptető modulok, és proximity kártyák kiválasztásánál elsődleges szempont volt kompatibilitás. Proximity kártyáink az olvasókkal egyező INDALA gyártmányú eszközök. Az INDALA kártyák bankkártya méretű közelítő (proximity) kártyák. A kártyákra könnyen készíthető színes, grafikus megszemélyesítés. A legtöbb fényképes azonosítókat készítő rendszerhez illeszkedik, melyek öntapadós fényképes matricát, vagy PVC overlay-t használnak. Az INDALA kártyaolvasó a labor bejáratának külső oldalára lett beépítve, mely összeköttetésben áll a faliszekrényben lévő andover vezérlővel.

A felsorolt eszközök vezérlését a laborban a hardverkulccsal ellátott CyberStation 1.81 es program irányítja. A programmal konfigurálhatjuk a beléptető rendszerünket, jogokat adhatunk, vonhatunk meg, és a biztonsági kamerák képeit is szintén ezzel igény szerint változtathatjuk.

6. A beléptető rendszer hálózata



15. ábra: Általános beléptető rendszer hálózati felépítése

A hálózati technológia kiválasztásakor a következőket kellett figyelembe venni: a számítógépek helye, a hálózat kívánt sebessége és a költségkeret. Erre a legmegfelelőbb választást az ethernet hálózata jelentette, amely tcp/ip – vel kommunikál a rendszer számítógépei között. Az iskola harmadik emeletén található szervergép és a laborban kialakított Cyberstation munkaállomás között a kommunikáció gyors és megbízható kommunikációját elősegítette még a hálózatba integrált BACnet protokoll.[10]

6. 1. *Kommunikáció a hálózaton*

Az Internet lokális hálózatokból épül fel. Sok kisebb nagyobb hálózatból, amelyeket routerek kapcsolnak össze. Ez azt is jelenti, hogy a hálózati kommunikáció azonos lokális hálózaton levő számítógépek között másképpen zajlik, mint az egymástól távoli, különböző lokális hálózatba tartozó számítógépek között.[10]

- **Lokális hálózat**

Lokális hálózatnak tekintendő az a hálózat, amelyen belül két számítógép között router közbeiktatása nélkül, közvetlenül lehet kommunikálni. Ez sok esetben egyetlen (koax) kábelt

jelent, de jelenthet hub-okkal, vagy switch-ekkel összekapcsolt koaxra vagy UTP kábelre kapcsolódó számítógépeket is. Szokás ezt szegmensnek vagy alhálózatnak is nevezni.

Több fajta hálózat típus is létezik (Token bus, Token ring, Ethernet, stb.) melyek közül most csak az Ethernet-re térnék ki, mivel a beléptető rendszerünk ilyen hálózattípust használ. Itt egy szegmensen, jellemzően egyszerre csak egy számítógép kezdeményezhet kommunikációt (adó). Ha valamelyik gép adni szeretne, akkor megvizsgálja, hogy szabad-e a kábel, ha igen, akkor használni kezdi. Persze még ekkor is előfordulhat, hogy többen egyszerre kezdik használni a kábelt, ilyenkor természetesen nem lehetséges értelmes kommunikáció - ezt hívják ütközésnek. Ezt az interface-ek (hálózati kártyák) felismerik, ekkor azonnal beszüntetik a forgalmazást, majd véletlen ideig várnak, és újra próbálkoznak.

Tehát egyszerre mindig csak egy gép forgalmazhat, viszont az üzenet szólhat mindenkinek (broadcast) illetőleg egy meghatározott címzettnek. Természetesen a csomagot elvileg minden gép látja (hiszen azonos kábelhez csatlakoznak) de csak az használja fel, akinek szól (illetve broadcast esetén mindenki). Hogy kinek szól, azt a címzett gép hálózati kártyájának fizikai címe (MAC address, Ethernet address, stb.) határozza meg. Ez a cím minden hálózati kártyára egyedi, és csak ennek ismeretében lehetséges két számítógép között kommunikációt megvalósítani.

Miért van szükség akkor az IP címre, miért nem használja a protokol a fizikai címeket?

Először is mert kényelmetlen, nehezen megjegyezhető. De ami sokkal fontosabb megváltoztathatatlan, ezért rugalmatlan, ami azt is eredményezi, hogy önmagában a címzett fizikai címének ismeretében nem vagy csak nagyon nehezen eldönthető, hogy a címzett az adott szegmensbe tartozik-e vagy sem, márpedig két számítógép egymással csak akkor tud közvetlenül kommunikálni, ha egy alhálózatba tartoznak.

Hogyan dönthető akkor el, hogy egy adott IP címmel rendelkező gépnek (címzett) mi a fizikai címe?

Erre szolgál az ARP (Address Resolution Protocol). Ha egy gép egy másikhoz akar kapcsolódni - amelyről a subnet mask alapján tudja, hogy vele azonos alhálózaton van -, akkor elküld egy broadcast üzenetet, amelyben megkérdezi, hogy ki is az XY IP címmel

rendelkező számítógép és mi is az ő fizikai címe. Az üzenetet mindenki veszi, de csak az válaszol rá, aki az adott IP cím tulajdonosa, és elküldi a kezdeményezőnek a saját fizikai címét (a kezdeményező a sajátját természetesen feltüntette az üzenetben). Ezután a kezdeményező - hogy ne kelljen folyton ARP üzeneteket küldözgetni - elhelyezi a címzettre vonatkozó információkat egy gyorsítótárba (ARP Cache) és legközelebb, ha ugyanazzal a címzettel akar kommunikálni, akkor már abból veszi az adatokat.[8]

- **Globális hálózat**

Mi történik akkor, ha olyan címzettel akar egy számítógép kommunikálni, aki nincs vele egy szegmensen?

Ekkor jut szerephez a router. A router (gateway, útválasztó) egy kitüntetett számítógép a szegmensen, amely egyszerre több lokális hálózathoz is kapcsolódik, és amelyik épp ezért több szegmensbe is tud adatot küldeni, így lehetővé teszi a szegmensek közötti kommunikációt. Ha egy számítógép egy másik szegmensben (ezt a subnet mask segítségével állapítja meg) lévő géppel akar kommunikálni, akkor nem közvetlenül a címzettel kezdeményez kapcsolatot, hanem az alapértelmezett útválasztóval (ez minden gép esetén be van állítva). Ehhez persze először ARP-vel kideríti a router fizikai címét, majd elküldi az adat csomagot, azzal az utasítással, hogy végeredményben az XY IP címre kell eljuttatni. Ezután ha a célcím valamely a router-hez kapcsolódó alhálózathoz tartozik (megint csak subnet mask), akkor ARP-vel kideríti annak a fizikai címét, és elküldi a csomagot. Ha a címzett egyik a routerhez kapcsolódó szegmenshez sem tartozik, akkor a router is egy másik - vele egy szegmensen levő - routerrel veszi fel a kapcsolatot, és annak küldi tovább a csomagot.

Fontos észre venni, hogy két számítógép között ebben az esetben is csak egy szegmensen belül, és a fizikai címek alapján zajlik a közvetlen kommunikáció, szegmenseken kívülre közvetetten (routerek közbeiktatásával) kerülnek a csomagok.[10]

6. 2. *Címzés*

A gépek egyedi azonosítására szolgál a címzés mechanizmusa. A jelen keretek között az IPv4-es szabvány kerül ismertetésre, mivel ez a legelterjedtebb IP szabvány. Az IPv6-os szabvány bevezetés alatt áll (IPv5 nem volt). A címek 32 bitesek a cím három részre osztható:

Előtag: Ez azonosítja a címosztályt. A címosztály mutatja meg, hogy az előtag után hány bitet kell hálózati címként, és hány bitet kell host címként értelmezni.

Network Adress (hálózati cím): Az egyes hálózatok megkülönböztetésére szolgál, valamint a központi adminisztrációt segíti elő, azaz ne lehessen két gépnek azonos IP címe. A hálózati címet központilag kell igényelni, és központilag utalják ki az igénylőnek.

Host Adress: A 32 címbit maradékát teszi ki. Ezt szabadon állíthatja be a címtartományt igénylő a saját gépein. [10]

Az idegen partícióvezérlő

A kontroller az idegen (külső), vagy más néven harmadik partíció rendszerbe illesztéséhez, telepítéséhez használt eszköz az épületautomatizálási- és felügyeleti rendszerben. A harmadik partíció berendezéseinek és rendszerének illesztését az automatikai szinthez BACnet-en keresztüli csatolással oldja meg a készülék, amely feltérképezi és ellenőrzi az idegen partíciót, legyen az HVAC, világítás, PLC, vagy más. Ezen felül protokoll funkciókkal rendelkezik, és szabadon programozható, mint egy automatikai állomás, de nem rendelkezik fizikai be- és kimenetekkel. Az ellenőrzést és kommunikációt a harmadik partícióval, egy program segítségével végzi. A készülék egyaránt rendelkezik egy BACnet (RJ45 csatlakozó, vagy csavart érpár csatlakozó) és egy soros interfésszel.

A rendszer topológiájában az eszköz három irányba kommunikál:

- a BACnet kommunikációjú LON buszon tart kapcsolatot a rendszer többi elemével;
- közvetlen kapcsolatban van a programot futtató számítógéppel;
- a harmadik partíció eszközeivel kommunikál adott buszon (pl.: Modbus, P-busz) keresztül

A hálózati csatoló

BACnet protokollal kommunikáló router a LON és az Ethernet hálózat között. Minden esetben alkalmazni kell, ha szükségünk van rá, hogy az automatikai állomások

kommunikáljanak Ethernet hálózattal is. Ekkor a vezérlők LON buszon kapcsolódnak egymással és a routerrel, amely BACnet Broadcast Management Device objektummal rendelkezik. Ez az eszköz az Ethernet hálózaton keresztül kommunikál a felügyeleti számítógéppel vagy egy másik routerrel, illetve azon keresztül más automatikai állomásokkal, vezérlőkkel. Egy statikus IP címet, egy alhálózati maszkot és egy alapértelmezett átjárót kell megadni minden egyes BACnet routernek az átjáró kiválasztása közben. A DHCP nem támogatott, a BACnet kommunikáció a statikus UDP porton keresztül történik. Az UDP port száma az átjárók kiválasztása során önállóan adódik. Maximálisan tíz BACnet átjárót lehet BBDM objektummal felruházni.

6. 3. *Buszrendszerek áttekintése*

Intelligensnek a gépi intelligencia terén azokat a készülékeket nevezzük, amelyek taníthatóak, azaz programozhatóan bonyolult feladatokat képesek elvégezni. A buszrendszerek fejlődésének kezdeti stádiumában csak központi intelligenciáról beszélhettünk, azaz a rendszerben csak egy központi helyen lévő vezérlőegység létezett. A mikroprocesszor-technika fejlődésével vált lehetővé, hogy olyan buszrendszerket fejlesszenek ki, ahol nincs központi vezérlőegység: az intelligencia szét van osztva az egyes készülékek között, méghozzá demokratikus módon, egyenlő arányban. Ezek az osztott intelligenciájú rendszerek. A buszrendszerek akkor működnek jól, ha az adatok időben egymás utáni átvitele olyan gyors, hogy az alkalmazás nem veszi észre a különbséget a buszrendszerű és a hagyományos, párhuzamos kábelezés között.

Minél több információt kell egyidejűleg átvinni a buszrendszeren belül, az annál igényesebb és drágább megoldást igényel. A költségtakarékos busz egyik legfontosabb követelménye, hogy csak annyi információt vigyünk át a buszon, amennyire feltétlenül szükség van.

A jeleket a vezetéken meghatározott sebességgel visszük át, amelynek mértékegysége ún. bit/s vagy baud. Az egyes buszrendszereket az átvitt adatmennyiségek és a reakcióidőket tekintve osztályokba sorolják. Jelenleg három, nemzetközi szabványokban rögzített szint létezik: terepi szint, automatizálási szint és menedzsment szint.

Terepi rendszerek esetében viszonylag kevés adatot kell egyidejűleg átvinni, azonban a reakcióidők igen rövidek.

Az épületoptimalizálási szolgáltatások terén (Building Automation Services) a három szintnek a következő feladatokat kell ellátnia:

Menedzsment szint: adatok analizálása, grafikus megjelenítése, dokumentálás, adatok archiválása, adatok/állapotok nyomtatása, telekommunikációs kapcsolatok (értékesítések telefonon, faxon, e-mail-ben, SMS-ben), riasztások kezelése, általános rendszerkezelés, tervezés, karbantartás, kezelői készülékek közötti adatkommunikáció biztosítása.
A menedzsment szintet a Ethernek hálózatra ültetett rendszerek uralják. Ezek a hálózatok egyre megbízhatóbbak és egyre nagyobb teljesítményűek. Az ilyen rendszerek egyre több feladatot vesznek át az automatizálási szinttől.

A busztechnika az iparban a következő területeken terjedt el:

- Gyártásautomatizálás
- Folyamatautomatizálás
- Épületautomatizálás
- **Biztonságtechnika és beléptetés vezérlés**
- Közműtechnika
- Környezetvédelmi felügyelet
- Gépek, készülékek egyedi aggregátorok belső vezérlése
- Repülőgépek, közlekedési eszközök belső vezérlése

Automatizálási szint: terhelés-menedzsment, időprogramok, logikai kapcsolatok, szabályozások, számítások (adatkonverziók) elvégzése, üzemórák számlálása, kézi működtetés, függvényekkel való műveletek, felügyelet, mérések elvégzése, technikai zavarjalak kezelése.
Az automatizálási szinten több programozható készüléket kötünk össze egy hálózattá. A készülékek egymás között cserélnek adatot. Magasabb szintű szolgáltatások, mint például programok készülékekben töltése is ezen az adathálózaton zajlik le.

Terepi szint: mérés, visszajelzés, kapcsolás, beállítás.

A terepi szinten néhány bit illetve bájt átviteléről van szó, azonban az adatok átvitelének a lehető leggyorsabbnak kell lennie. Az elvárt reakcióidő 50 ms között van. Az ezen a szinten üzemelő buszkészülékeknek egyszerűen kezelhetőnek.

A három szint osztályozásába besorolt leggyakrabban alkalmazott buszrendszerek:

Menedzsment szint: (rendszerbuszok)

- PROFIBUS-FMS (EN szabvány)
- WorldFIP (EN szabvány)
- P-NET / (EN szabvány)
- INTERBUS (EN szabvány-tervezet)
- Modnet/Modbus
- ARCNET
- FOUNDATION Fieldbus (IEC-Mezőbusz-szabvány)
- BACnet (ANSI, EN szabvány)

Automatizálási szint: objektumközeli rendszerbuszok

- PROFIBUS-DP (EN szabvány)
- PROFIBUS-PA (EN szabvány)
- DIN- Messbus
- SERCOS (EN szabvány, IEC szabvány)
- BITBUS (IEEE-szabvány)
- CAN (ISO- szabvány)
- LON (IEC szabvány-tervezet)
- EIBnet (EN szabvány-tervezet)

Terepi szint: (Szenzor-Aktor buszok)

- AS-Interface (IEC- szabvány- terv.)
- INTERBUS-Loop
- HART
- EIB (EN szabvány)
- M-BUS (EN szabvány)
- LCN [8]

6. 4. *Bacnet:*

A BACnet lényege tulajdonképpen abban áll, hogy a különböző funkciójú és gyártójú készülékek közötti kapcsolatot két számítógép közötti kapcsolatra redukálja, amely egy hálózat közbeiktatásával jön létre. A protokoll teljesen elszakad az OSI referenciamodell fizikai rétegétől, azaz az átviteli médiumtól. A BACnet szempontjából teljesen lényegtelen, hogy a készülék milyen belső felépítésű és milyen szoftver fut benne. A készülék a hálózat felé az objektumon keresztül tartja a kapcsolatot.
A BACnet további előnye a többi protokollal szemben, hogy összeolvad a menedzsment és az automatizálási szint. A vezérlő állomás és a DDC (Direct Digital Control) modulok közötti kommunikáció például az automatizálási szinthez tartozik, míg igazi menedzsment kommunikáció csak a menedzsment munkaállomások és kezelőkészülékek között zajlik. A BACnet támogatja a távmenedzsment lehetőségeket is (Internet, WAN) lehetővé téve nagyobb távolságok áthidalását is. A buszterhelés csökkentése érdekében a BACnet eseményvezérelt, ami azt jelenti, hogy adatátvitel vagy ciklikusan vagy/és az értékek, megváltozásakor van.
Különböző átviteli sebességű és topológiájú hálózatok BACnet routereken keresztül összekapcsolhatóak

Piaci elemzők szerint a BACnet protokoll jó úton halad afelé, hogy rövidesen világméretű szabvánnyá váljék az épületoptimalizálás menedzsment szintjén, amely a különböző gyártóktól származó különböző terepi eszközöket összefogja. A BACnet egyesíti magában az eddigi épületfelügyeleti protokollok előnyeit azok hátrányainak elhagyásával. A BACnet támogatja a legkülönbözőbb transzport protokollokat, mint pl. az Ethernet, Arcnet vagy LonTalk. Az átviteli médium lehet csavart érpár, fénykábel, erősszámú hálózat, rádiófrekvencia, infravörös átvitel vagy telekommunikációs hálózat. Az egy átivteli médiumok egyszerű routerekkel kapcsolhatóak össze.

6. 5. *Lonworks rendszer*

A LONWORKS hálózat maximum 32 385 intelligens buszrésztvevőből, csomópontból állhat, amelyek a LONTALK protokoll szerint egységes nyelven

kommunikálnak egymással. Egy hálózaton belül maximum 255 vonal alakítható ki. Az átviteli sebesség maximum 1, 25 Mbit/s lehet, de az Ethernet felhasználásával, mint gyors backbone (gernic), az átviteli sebesség tovább növelhető. Az Internet technológia felhasználásával a Lonworks hálózat tetszőlegesen kiterjeszthető. Az épület adataihoz a világ bármely pontján hozzá lehet férni, és olyan vállalatok, amelyek több telephellyel rendelkeznek egysége, integrált hálózattal láthatók el.

LON – az épületautomatizálás buszrendszere

Egy univerzálisan alkalmazható automatizálási rendszerrel szemben magasak a követelmények. A LON - technológia egy olyan hálózat, amely kielégíti ezen követelményeket.

- A LON topológiája és rendszer-felépítése kimondottan épületautomatizáláshoz lett kifejlesztve.
- Minden szokványos adatátviteli közeg – sodrott érpár, táphálózat, rádiófrekvenciás-, infravörös- és üvegszál-technológia – használható.
- A LON egy nyílt, több-beszállítós, szabványosított rendszer. Világszerte több mint 3000 cég gyárt LON termékeket, ezek 45%-a társítható az épület-automatizálás területéhez.
- A LON felöleli a kommunikáció minden szintjét, kezdve a terepi eszközöktől, át az automatizálás szintjén egészen a felügyeleti szintig.
- Mivel a LON nem központosított rendszer, a működési megbízhatósága magasabb, valamint sokkal összetettebb rendszerek hozhatók létre. Továbbá, az elosztott intelligencia megkönnyíti a kezelést, az átláthatóságot és növeli az elrendezési lehetőségeket.
- A LON készülékek egymással együttműködnek. A különböző gyártók termékei összeköthetők, így összekapcsolásukkal új funkciók jöhetnek létre.
- A LON egy szabványosított rendszer. Néhány éve a LON szabványosítva lett az ANSI/EIA/CEA-709 alatt, az „IP-alapú LON” pedig az EIA/CEA 852 alatt. Az európai szabványosítás az EN14908 szabvány szerint történt meg. [8]

7. A TAC szoftver bemutatása

A TAC nyílt, szabványos technológiája lehetővé teszi, hogy egy rendszerbe integrálja a fűtés, hűtés, beléptető-, vagyonvédelmi, szellőztető, tűzjelző és világításvezérlő rendszerét a teljes vállalatára vonatkozóan. Ez a megközelítés lecsökkenti a képzési és oktatási költségeket, növeli az energia megtakarítást és a létesítményére vonatkozó releváns adatok összegyűjtésével, és megosztásával lehetővé teszi annak még gazdaságosabb üzemeltetését. A teljes irányítás az egyén birtokába kerül az egész épületre – vagy akár több épületre, vagy akár mindenegyes épület minden egyes helyiségére– vonatkozóan, egyetlen felhasználói interfészen keresztül. A könnyebb irányítás megtakarítást, rugalmasságot, biztonságot, kedvezőbb tulajdonságokat és felhasználó barátüzemeltetést nyújt. A kedvezőbb klímaviszonyok mellett még a dolgozói hatékonyság is nőhet. A nyílt rendszerek emellett szabadságot nyújtanak az új, innovatív megoldások létrehozásában is. Mivel szabványos technológiát használ– TCP/IP, LonWorks, BACnet és Ethernet –, a megoldások a piacon lévő összes rendszerrel kompatibilisek és egy hálózatba integrálhatóak. Ez nagyobb választási lehetőséget biztosít és megvéd attól, hogy végérvényesen „beragadjon” egy beszállító rendszerébe. [11]

7. 1. *Continuum CyberStation 1. 81*

Az Andover Continuum CyberStation munkaállomás szoftvere egy Microsoft Windows alapú, színes, grafikus felhasználói felület. A Continuum szoftvere hatékony szolgáltatásokat és időtakarékos eszközöket nyújt az Andover Continuum intelligens épületautomatikai rendszer vezérléséhez, megjelenítéséhez nagy sebességű Ethernet LAN/WAN vagy egy munkaállomásos környezetben.

A CyberStaion 1. 81 – s verziójú szoftvercsomagot használja a szakdolgozatban tárgyalt K/7 – s terem is, amely kontrollálja és felügyeli a felszerelt beléptető rendszert.

Az egy munkaállomásos verzió (Single User – SU) egy Windows munkaállomást futtató PC-ből áll. A telepítő CD telepíteni fogja az MSDE adatbázist és az Andover Continuum szoftvert. Az Andover Continuum felhasználói felületéről irányíthatja az épületét. Egyetlen Andover Continuum munkaállomásról központilag irányítható az épület, amely mint egy láthatatlan rendszer összegyűjti az épület által generált információkat. Az Andover

Continuum grafikus menürendszeren keresztül jeleníti meg az információkat a létesítményéről. Riasztások megtekintése és nyugtázása, személyek követése, ajtók nyitása és zárása, világítás fel-le kapcsolása, alapjelek módosítása, berendezések ki-be kapcsolása, jelentések készítése, időprogramok módosítása, naplózott adatok megjelenítése válik lehetővé többek között a munkaállomás szoftver segítségével. Kis rendszerek esetén, azaz maximum 3 munkaállomás alkalmazása esetén még nem szükséges az önálló fájlszerver telepítése (CyberStation 1. 5 verziótól). Ekkor még használható az egy munkaállomásos rendszer MSDE adatbázisa. Ilyen rendszerkonfiguráció lehet például: 1 x SU (programozói verzió) + 1 vagy 2 x LAN verzió. Az SU fogja helyettesíteni a fájlszervert és annak az MSDE adatbázisa lesz megosztva a maximum 3 db munkaállomás között. Az ilyen rendszerek adatbázisának megengedett maximális mérete 2 GB, ha az adatbázis ennél nagyobbra nő, akkor a rendszert hálózati, más néven több munkaállomásos verzióra kell felfejlesztetni, és ebben az esetben önálló fájlszerverre is szükség van. A több munkaállomásos rendszerekben az Andover Continuum felügyeleti program egy Microsoft ODBC kompatibilis adatbázisban tárolja a létesítményből származó naplózott energiafogyasztási, karbantartási, biztonságtechnikai adatokat, riasztásokat és eseményeket.

Az SQL az adatbázisok ipari szabványa, amely egyben azt is jelenti, hogy a Continuum képes az adatait a meglévő rendszerekkel és hálózatokkal megosztani. Az információk az illetéktelen hozzáférésektől egy kifinomult, de a felhasználó által konfigurálható „kulcs” segítségével védettek. Az egyedi kulcsok a szoftver különböző részeit képesek „felnyitni”, például: objektumosztályokat, tevékenységeket és egyedi objektumokhoz való hozzáférést. A rendszer adminisztrátora osztja ki ezeket a virtuális kulcsokat, vagy más néven hozzáférési jogokat a szoftver különböző részeihez való hozzáféréshez. Az Andover Continuum munkaállomása alkalmazások sorát tartalmazza, melyek a háttérben láthatatlanul működnek együtt egymással. Az OLE (objektumkapcsolás és -beágyazás) automatizáció az adatokhoz való hozzáférést teszi lehetővé olyan alkalmazásokon keresztül, mint a Microsoft Word, Excel, Netscape Navigator és Visio.

7. 2. *Web.Client*

A TAC Web.Client szoftvere a jogosultsággal rendelkező személy számára hozzáférést biztosít az épületmenedzsment rendszeradataihoz egy hálózatba vagy internetre csatlakozó, web böngészővel rendelkező normál PC-ről. Ez jelentős előnyöket biztosít az

integrált épületmenedzsment rendszer számára. A jogosultsággal rendelkező felhasználó módosíthatja a helyiség-hőmérsékleteket, szabályozhatja a kártyás beléptetést, megtekintheti a kameraképeket, nyugtázhatja a riasztásokat, módosíthatja a foglaltsági táblákat anélkül, hogy ehhez dedikált munkaállomásra lenne szüksége. A rendszer integritásának fenntartása érdekében a Web.Client is jelszóvédett. A rendszert úgy tervezték, hogy a felhasználó könnyen és gyorsan jelentkezhessen be a rendszerbe, megtekinthesse a szükséges adatokat, majd elvégezhesse a jogkörébe tartozó tevékenységeket.

- gyors hozzáférés a rendszerhez
- a vezérlési és biztonságtechnikai döntéseket a lokálisan érintettekhez delegálja
- könnyen használható és biztonságos interfész
- előre konfigurált, könnyen hozzáadható meglévő Continuum rendszerekhez

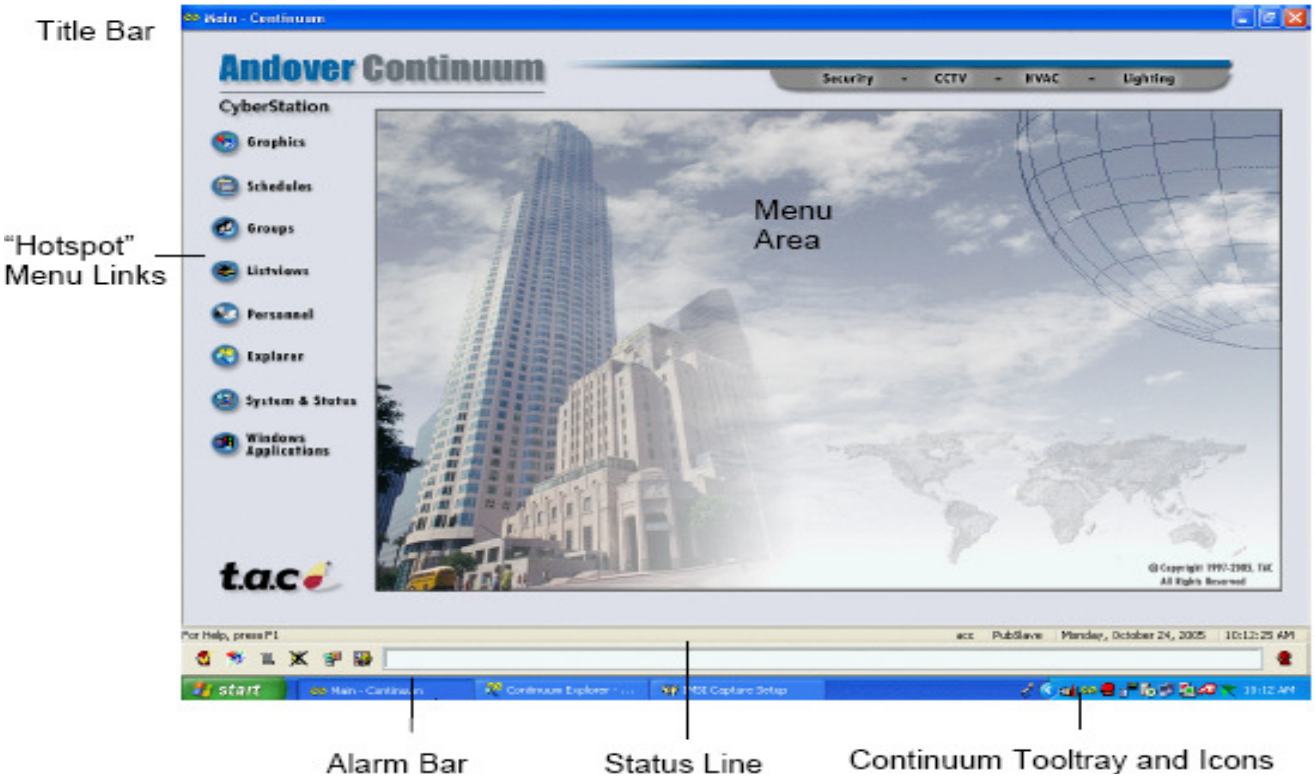
7. 3. *A CyberStation indítása*

A programok listájából való indítás után egy beléptető ablak jelenik meg amelyben a szoftver a jogosultság ellenőrzését végzi – felhasználói név – jelszó formában.

16. ábra: Cyberstation beléptető ablaka

A megadott felhasználónév és jelszó ellenőrzése után a program ellenőrzi annak helyességét és vár a beléptető folyamat megszűnésére.

7. 3. 1. *A CyberStation főmenüje*



17. ábra: A CyberStation főmenüje

A program indulását követően a főmenü fogad minket, amely segítségével tudjuk a beléptető rendszerünket teljes körűen használni, és új belépési jogokkal felruházni egyes felhasználókat. Ebben a fejezetben bemutatom a program működését, és az első indulás alkalmával kötelezően elvégzendő konfigurálását, amely elengedhetetlen a hibátlan működés érdekében.

A főmenünek 5 alapvetően elkülönülő blokkját különböztetjük meg az alábbiak szerint:

- címsáv
- menü terület – A státusz sor és a címsor között elhelyezkedő terület
- főmenü linkek vagy "kritikus helyek" - jelenítik meg a menüből elérhető főbb funkciókat:

  Grafikai beállítások - A program futása közben tárolt jegyzékek elérése – A felhasználói csoportok elérése – A programban tárolt listák hozzáérhetősége – Személyes beállítások – a rendszer állapotának megjelenítése–Windows alkalmazások listája.
- Status Line - Információkat jelenít meg a felhasználóról, úgymint név, munkahely neve, aktuális dátumot és az időt, hibaüzenetek megjelenítésére is alkalmas.
- Riasztás Bár – Szöveget jelenít, meg amely leírja az aktív riasztási állapotot.

Minden CyberStation menüpont ugyanazokkal az alapvető funkciókkal rendelkezik, mint a főmenüje a programnak.
Alapvetően két féleképpen választhatunk elemeket a CyberStation főmenüjéből:

- úgynevezett „hotspot links” és
- felbukkanó menü (Popup menus) formájában

Hotspot linkek:
A választható menüpontok együttese a menü oldalon. Ezekre az elérhetőségekre kattintás után a program viselkedése, és navigálása a következőképpen alakulhat:

- a folyamat, amelyet elérni szeretnénk egy új oldalon, folytatódik
- egy meglévő program futtatása, konfigurálása
- új objektumok létrehozása a programban

A CyberStation menüpontjai, mint gombok tűnnek fel a menüben, és egyértelműen meghatározza őket szöveges beszélőnevük. Adott esetben ikonokkal vannak ábrázolva, illetve azok egyszerű tárgyakként, mint például ajtók, kazánok, illetve vezérlők vannak feltüntetve. Tehát a programnak van teljes grafikus felületen ábrázolt, csak objektumokat használó grafikus része. A felhasználó tudja, ha ezekben a menükben vándorol, a kurzor jelzi neki a változtatásokat, mégpedig úgy hogy a menüben eddigi nyila szimbólum kézre vált.

A CyberStation főmenüjéből elérhető fontosabb funkciókat, amelyek mind az épületfelügyeleti rendszert hívattak könnyebb kezelhetőséggel felruházni. A K/7 – s labor hibátlanul működő belépető rendszere bizonyíték arra, hogy ez a program teljes körű felügyeletet biztosít, és átláthatóságával a most piacon lévő felügyeleti rendszerek egyik legjobbja.
Minden menüpont a szoftver külön képességeit jeleníti meg. Teret adva az épületautomatizálási rendszer éppen tárgyalt részének kontrollálhatóságára.

7. 3. 2. *Graphics menü:*

A Cyberstation munkaállomás ezen menüpontjában, különböző grafikus alkalmazásokat használhatunk egyes szimulációk előállítására. Egyfajta dinamikus, virtuálisan modellezett vezérlőpultokként funkcionálnak.

A CyberStation segítségével modellezhetjük, és teljes mértékben legenerálhatjuk a valóságban létrehozott rendszert. A számítógép ellenőrző logikai paneleket generál már meglévő fizikai panelekből. A modellben ábrázolhatjuk a rendszer működéséhez elengedhetetlen összetevőket: gombokat, kapcsolókat, animációkat, és a rendszer milyenségétől függően más fizikai összetevőit a rendszernek.

Elengedhetetlen egy épületfelügyeleti rendszer tervezésénél hogy ellenőrzési pontokat hozzunk létre, amely tárolja az összes fontos rendszerváltozók tulajdonságát, vagy bizonyos Continuum elemek, esetünkben a területek és az ajtók beállításait. Minden ellenőrző pont, amit a CyberStation - ban helyeztünk el könnyen változtatható, a törlés a megfelelő prioritással rendelkező felhasználónak direkt megoldható a szoftveren keresztül.

Az ellenőrző pontok a szoftverünkben, két állapotban lehetnek: aktív és passzív.

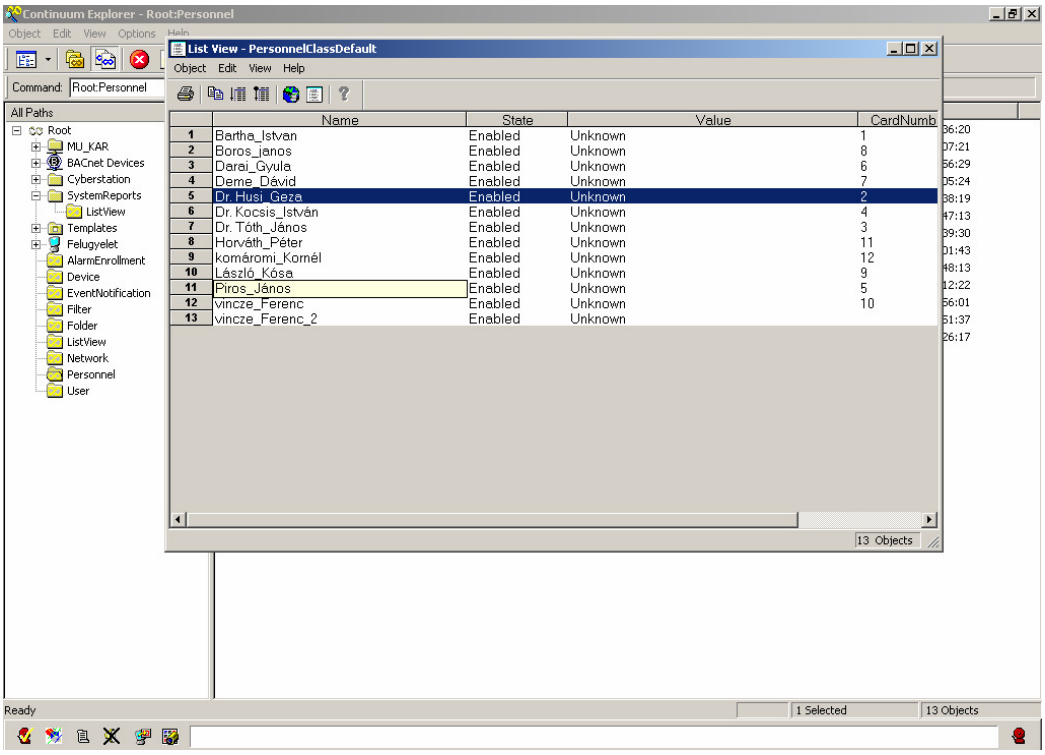
• aktív ellenőrzéseknek nevezzük a kapcsolót vagy gombot, mert azt valósidőben egy felhasználó kezeli.

• a passzív ellenőrzések feladata az információközvetítés. A műszereken mért adatok megjelenítése a felhasználó felé, továbbá a csak olvasható ellenőrzésekkor keletkezett naplók tárolása és adott környezetben „ad- hoc” előhívása. A létrehozott vezérlőpulton lehet egy vagy több ellenőrzési pont, de ha a biztonsági előírások előírják, egy rendszernél előfordulhat, hogy minden a rendszerben elhelyezett objektumnak külön testre szabott ellenőrzési pontot kell definiálni.

7. 3. 3. *Groups menü:*

Ezen a lapon vihetjük fel a felhasználók csoportjait. A csoportba rendezésnek nagy gyakorlati előnye abból származik, hogy a jogosultságok beállítását, illetve a naplófájl szűrését nem kell személyenként elvégeznünk, hanem a csoportokhoz rendelhetünk jogosultságot, illetve beállíthatunk szűrőt. A szűrők beállításaira is számos lehetőség van, egyet megneveznék ezek közül: pl.: adhatunk jogosultságot csak hétvégi belépésre az egy csoportban szereplő felhasználóknak, amely időkorlát bármikor megszüntethető és módosítható.

7. 3. 4. Listviews



18. ábra: Listviews

A listview célja a continuum cyberstation szoftverében hogy információkat jelenít meg az adatbázisban tárolt objektumokról. A CyberStation adatbázisában tárolt felhasználókról megtudhatjuk a listából a nevüket, a tulajdonukban lévő kártya státuszát, amely kétféle lehet: Engedéllyel rendelkezik vagy engedély megtagadva. Továbbá a belépésükhöz szükséges belépőkártya számát. A programban testre szabhatjuk a megjeleníteni kívánt listákat, és szűrési feltételeket állíthatunk be, az adatok megjelenítését illetően. Törölhetünk a listából, és a create view – választahtó menüponttal új listát hozhatunk létre, amelyet ha akarunk html formátumba ment a program és a programban beépített nyomtató segítségével egyszerűen nyomtatja ki, a kívánt tartalmat.

Ebben a fejezetben a beléptető rendszer szoftverének lényegi részét, és annak beállításait mutatom be. A IAS automatika biztosítja a felhasználót különböző beléptető szintek létrehozására, ami magában foglalja a mágneskártyák egyedi programozását a felügyeleti szoftver segítségével.

7. 4. *Personnel menüpont*

A Personnel menüjéből két fő szoftverperiféria érhető el a Personnel Manager és a Personnel import utility. A CyberStation Személyzeti Managere egy erőteljes és könnyen használható eszköz, amely segítségével megtekinthetjük és gyorsan, és egyszerűen módosíthatjuk az eddig létrehozott személyzeti nyilvántartásunkat a rendszerben. Az Import segédprogram lehetővé teszi külső személyi adatok importálását a rendszerünkbe, amely egy Andover Continuum rendszeren kívül jött létre. Egyszerűen hozzáférhetők lesznek az adatok, nem lesz szakadék a két rendszer között. Ezzel kiküszöbölve más személyi adatbázisok és nyilvántartások lassú bevitelét a programba. A nagy mennyiségű adatbázisok és személyi rekordok gyorsan és problémamentesen importálhatóak, amelyek a CyberStation személyek objektumai közé kerülnek importálás után.

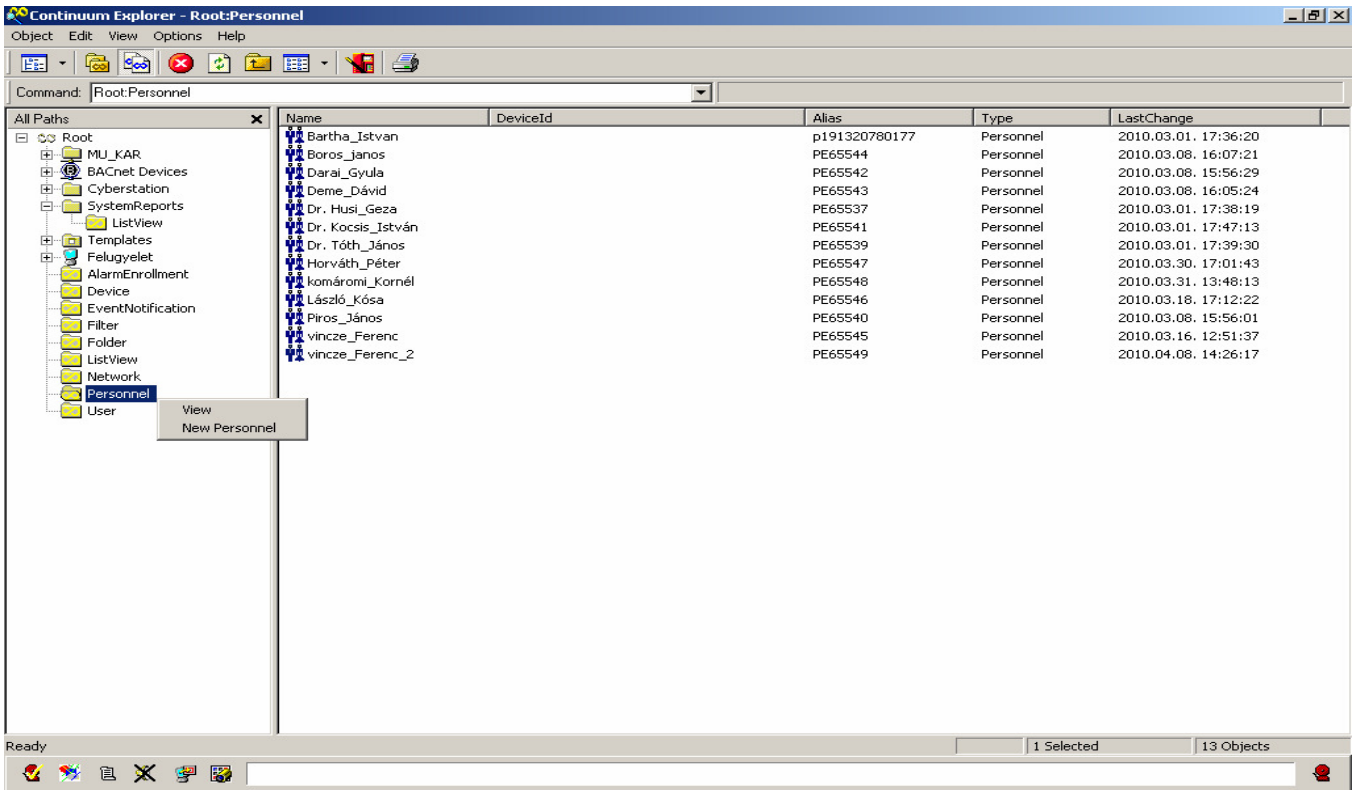
7. 4. 1. *Personnel Manager*

A dolgozatomban tárgyalt beléptető rendszerhez a legfontosabb szoftverelem, amely biztosította számunkra, hogy a meg lévő mágneskártyák tartalommal legyenek ellátva és kommunikálva az ajtónál lévő beléptetők a CyberStation szoftverrel, a megfelelő jogosultsággal rendelkező személyeket engedjék be a laborba.
A Managert használhatjuk belépő adatok megtekintésére, kezelésére valamint tárolására. A tárolható személyes adatok a következők:
• biztonsági információkat jelenít meg a beléptető kártyáról, mint például a kártyaszám, és megnevezésre kerülnek azok a területek, amelyek hozzáférhetők az adott kártya felhasználásával.
• felhasználási feltételek szerint tárolhat munkavállalói – munkáltatói adatokat, információkat, mint például a szervezeti egység nevét és törzsszámát, felügyelő szerveik neveit és elérhetőségeit, adott esetben járművek információit
• a személyes adatok a kártyát használó felhasználóról, mint például név, vércsoportja, segélyhívás esetén kapcsolattartó megnevezése, magasság, testsúly és akár a haj színét is képes tárolni a program.

Az előbbiekben felsorolt adatokat megtaláljuk minden felhasználónak a saját kártyájához tartozó személyi rekordjában.

A CyberStation Personal Managere és főbb funkciói:

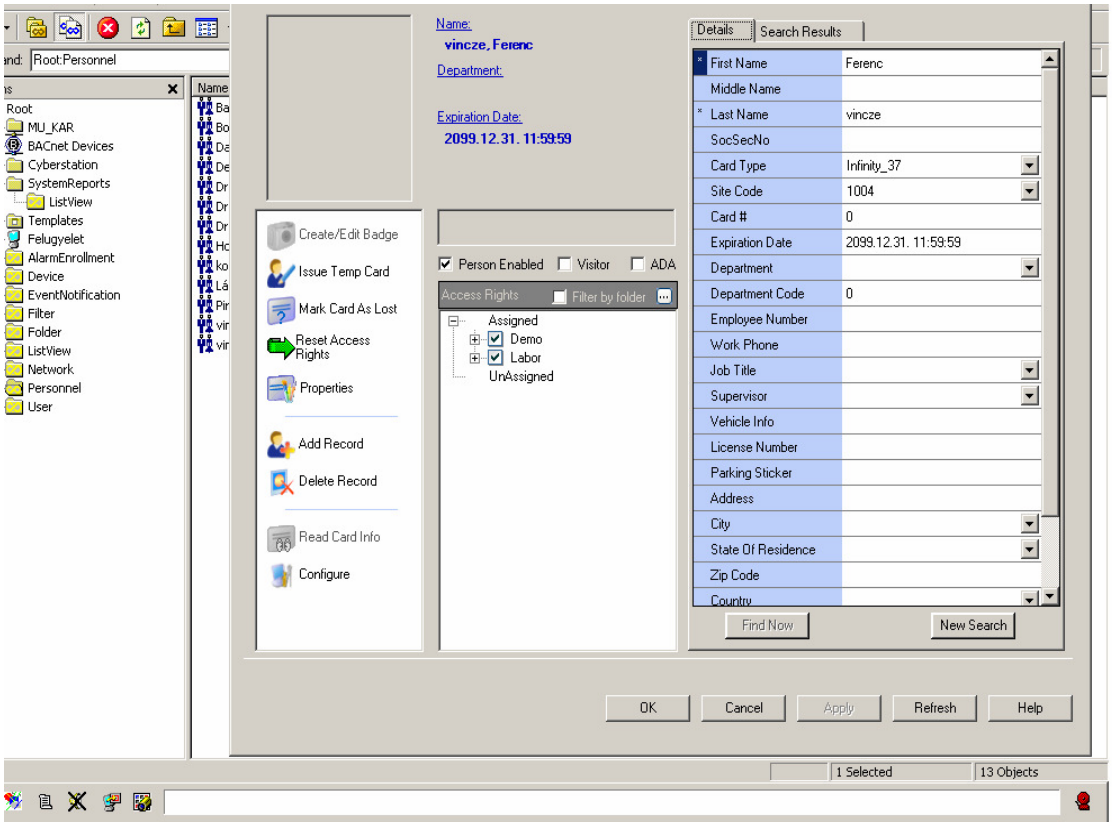
A főmenüből a már tárgyalt „hot-spot” menüpont segítségével érhető el az alap adatbázis részét képező Personnel menüje. A Continuum kezelőfelülete alapjaiban véve két részre tagolódik. Baloldalon egy faszerkezetű listaállományt találunk, amelyekből elérhetők a főbb funkciók. Jobb oldalon az eddig letárolt felhasználók listáját láthatjuk, amelyek belépési jogosultsággal rendelkeznek a K/7-s laborba. Láthatjuk a felhasználó nevét – aliasat[1] – felhasználási státuszát – és az utolsó módosítás időpontját a személyes rekordjában.
A listaállományban találhatóak a BACnet hardver eszközök, riasztási listák, és a hálózatra vonatkozó menüpontok, amelyeket a későbbi fejezetekben tárgyalok. A felhasználók adatait egyszerűen megtekinthetjük és módosíthatjuk, ha jobb klikkel rájuk kattintva a view felugró lehetőséget választjuk.



19. ábra: Continuum Explorer előlnézete

Új felhasználó hozzáadása a rendszerhez:

Egy új felhasználó hozzáadását a rendszerhez, amely belépési jogosultsággal fog rendelkezni saját proxy kártyájával a CyberStation beléptető rendszerében valósíthatjuk meg. A Personnel listaelemre jobb egérgombbal kattintva, válasszuk a New Personnel felugró menüt. A megjelent ablak a következő:



20. ábra: New personnel view

Itt tudunk az új felhasználónknak új rekordot létrehozni, és a rendszer rendeltetésének megfelelően a szükséges információkat tárolni. Mivel ez egy labor beléptető rendszere, amely nem rendelkezik munkaidő nyilvántartó bővítő modullal és a biztonsági előírások sem érik el a közepesnél magasabb szintet a program alapvető funkciói közül sem használtjuk fel az összes lehetséges alternatívát. Láthatjuk, hogy a megjelent menüben számtalan lehetőség nyílik egy felhasználó azonosítására. A kötelezően megadandó információk a következők:

- vezetéknév
- keresztnév
- a belépő kártya típusa
- site code

- a kártya száma
- a kártya lejárati dátuma (A 20. ábrán látható lejárati dátumot a program generálja)

Továbbá meg kell adnunk, hogy a felhasználó személyzeti vagy látogató státuszba kap engedélyt a laborba lépéshez. Amikor egy objektummal bővül a Personnel manager listája a CyberStation automatikusan generálja az object ID, és aliast, amelyeknek Continuum Explorerben megnyitásakor a felhasználókhoz lesznek rendelve.

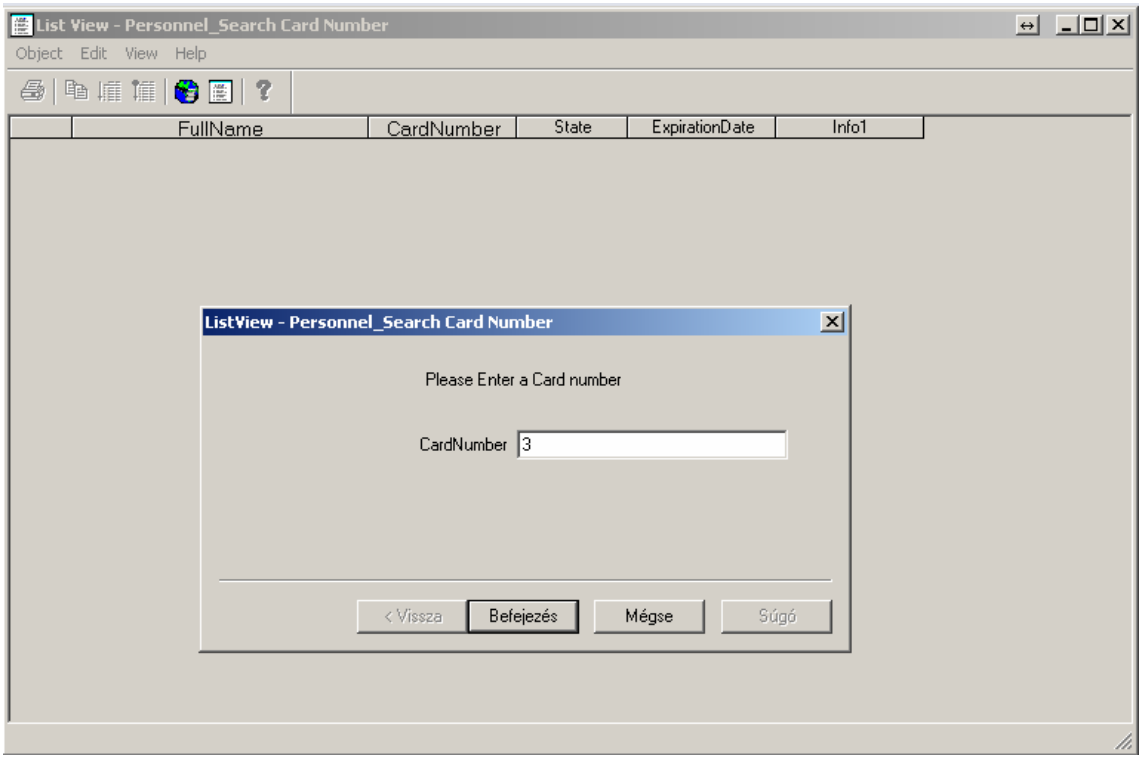
Keresés a managerben:

21. ábra: Keresési funkciók a managerben

A Personnel Manager segítségével gyorsan megtalálhatjuk a már letárolt személyek rekordjait a programban lévő beépített keresési funkció segítségével. Ezt a funkciót a „New search” ikonra kattintva érhetjük el. Keresési szempontok különbözőek lehetnek, mint vezeték és keresztnév, tulajdonos kártyaszáma vagy akár a lakóhely is ilyen szempont lehet az adatok hiányosságától függően. Megadhatja a teljes vagy részleges információhalmazt keresési kritériumnak.

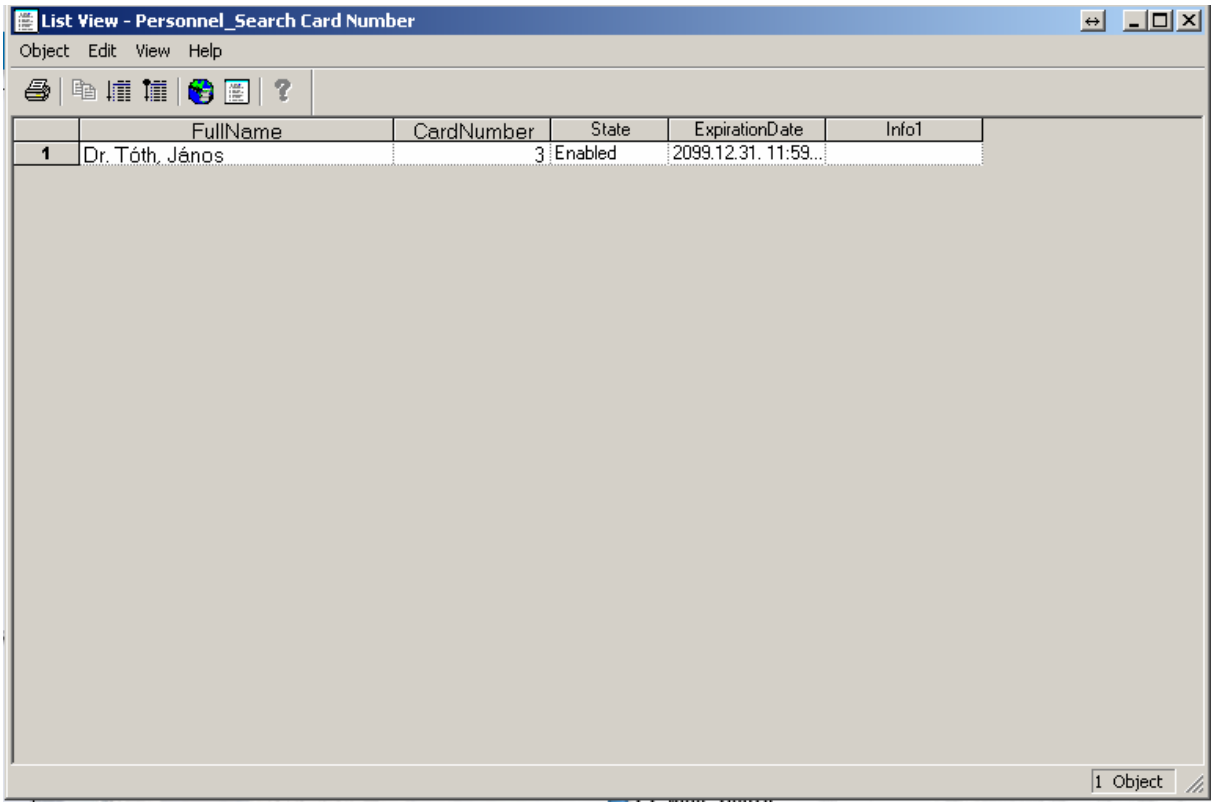
Keresés kártya száma alapján:

A főmenü personnel menüpontjára kattintva a 21. ábrán látható képernyő jelenik meg előttünk amelyben válasszuk a Card Num. Search menüpontot. Ekkor a következő képernyő fogad minket:



22. ábra: Keresés a personnelben kártyaszám alapján

Itt megadhatjuk a keresni kívánt kártya számát, amely segítségével a keresett személyhez társított kártyát a program keresni kezdi a tárolt listákban. Befejezésre kattintva, ha van a keresési kritériumnak megfelelő rekord az adatbázisban, akkor a következő formában láthatjuk:



23. ábra: Keresési eredmények a personnelben

Esetünkben a cyberstation adatbázisában a hármas sorszámú kártya Dr. Tóth János Tanár Úrhoz tartozik. A megjelenített adatokból megtekinthetjük a kártya státuszát és a lejárati dátumot.

A 20. számú ábrán láthatjuk a bal oldali menük és a kitöltendő személyes adatok táblázata közötti fehér területet, amely a programban definiált beléptetővel ellátott ajtókat szimbolizálja. Láthatjuk, hogy mind a demo mind a labor jelölőnégyzet be van jelölve, tehát a két beléptető aktív. A labor rész az ajtónál lévő külső és belső beléptető modult foglalja magába, amely már a programba letárolt kártyák hatására nyitja a labor bejáratot. A demo rész egy virtuális ajtót jelent, amely csak a kártyák próbájára hivatott, és amellyel a rendszerhez csatlakozva elérhetők az azonos funkciók, mint a konkrét ajtó esetében .

7. 4. 2. Personnel import utility

A Personnel import utility segítségével más rendszerekben létrehozott adatbázisokat ültethetünk át a programunkba, ezzel elkerülve a felesleges és időigényes letárolási mechanizmusokat.

8. Video megfigyelő rendszerek

8. 1. *Bevezetés*

A videó megfigyelő rendszerek napjainkban egyre nagyobb szerepet kapnak a riasztó és beléptető rendszerek mellett a komplex vagyonvédelemben. Ennek megfelelően a velük szemben támasztott igények is olyan mértékben megnőttek, hogy azokat hagyományos (analóg) rendszerekkel már nem, vagy csak részben lehet kielégíteni.
Jelen fejezetben azt mutatom be, hogy milyen feladatok megoldását várhatjuk el egy korszerű video megfigyelő rendszertől, milyen a jelenleg megvalósítható műszaki színvonal, a rendszerek tudása.

8. 2. *A video megfigyelő rendszerek elemei*

A biztonságtechnikai piacon jelenleg egyaránt megtalálhatóak az analóg és a digitális video megfigyelő rendszerek. Kettejük „versenyfutása” egyre inkább eldőlni látszik a számítógép alapú digitális rendszerek javára.

A rendszer főbb alkotóelemei:

- képalkotó eszközök (kamerák) különböző típusai
- videojel továbbítására szolgáló eszközök (konverterek, átjátszók)
- képfeldolgozó eszközök, képdigitalizáló (grabber) kártyák
- képkiértékelést, megjelenítést, tárolást végző szoftver

- a rendszert működtető számítógép

8. 2. 1. *Képalkotó eszközök*

Néhány évvel ezelőtt még igen behatárolt választéklistából lehetett az adott funkcióra legmegfelelőbb kamerákat kiválasztaniuk a telepítőknek és természetesen a végfelhasználóknak. A jelenlegi kínálatot vizsgálva azonban megállapítható, hogy éppen fordított a helyzet, hiszen szinte minden igényre létezik célzott megoldás. Digitális video megfigyelő rendszerek esetén, ha gyengébb minőségű, kis felbontású kamerákat alkalmazunk, akkor eredendően megfosztjuk a rendszert az egyik legfontosabb tulajdonságától, a nagyfelbontású, pontos azonosítást lehetővé tevő képek készítésétől. (hiába képes egy digitalizáló kártya 768x576-os felbontású képek digitalizálására, ha csak egy 280 soros kamera képeit kapja). Elérhető áron léteznek már olyan kamerák is, amelyek a nagy képfelbontáson túl, számos olyan paraméterrel rendelkeznek (pl.: nagy érzékenység, infraszűrő, táv vezérelhető paraméter-beállítás, automatikus üzemmód váltás), amelyekkel a digitális video megfigyelő rendszerek, által nyújtotta lehetőségek maximálisan kihasználhatók. Érdemes figyelmet szentelni a kamerák legújabb családjának az úgynevezett „Intelligens kameráknak”. Ezek az eszközök ötvözik magukban az analóg képalkotás minőségi jellemzőit, valamint a mikroprocesszor alapú jelfeldolgozás lehetőségeit. Kommunikációs buszon keresztül (pl. LON) képesek folyamatos kapcsolatot tartani a video megfigyelő rendszerrel és úgy módosítani paramétereiket, hogy az eltárolt képek minőségi jellemzői a legjobbak lehessenek. Természeten mindemellett lehetőséget biztosítanak arra is, hogy a kezelő a számára legmegfelelőbb beállításokat eltárolja, s a későbbiek folyamán ezeket bármikor visszatöltse.

8. 2. 2. *Videojel továbbítására szolgáló eszközök (konverterek, átjátszók)*

A kamerák által elkészített videojel eljuttatása a képfeldolgozó eszközökig nem minden esetben könnyű feladat. Szerencsésnek mondhatóak azok az esetek, amikor jeltovábbítás megoldható normál 75Ω-os koaxiális, vagy UTP kábelen keresztül. Számos olyan helyzet van azonban, amikor a kábelek kihúzása nem megengedett, vagy az áthidalandó

távolság igen jelentős mértékű. Ezekben az esetekben speciális jelátalakító eszközökre van szükség, amelyek a következők lehetnek:

- RF videojel átalakító
- optikai jelátalakító
- csavart érpáras videojel konverter

A videojel rádiófrekvenciás átvitelét biztosító eszközök sajnos csak korlátozott számban állnak jelenleg rendelkezésre. A tapasztalat azt mutatja, hogy alapvetően ezeknek két típusa létezik: az olcsóbb megoldások, amelyek csupán néhány méteres távolságig alkalmazhatók jelentős minőségromlás nélkül, és az igen nagy költségvonzattal járó eszközök, amelyek azonban akár több 10 kilométeres távolság esetén is megbízhatóan működnek (pl. a szórt spektrumú videojel átviteli eszközök). Az optikai képtovábbítás előnye, hogy igen nagy távolságokat is szinte minőségromlás nélkül át lehet vele hidalni. Azonban ez a megoldás is igen jelentős befektetéseket igényel, hiszen üvegszál kábeleket kell behúzni és minden egyes kamerajelhez szükséges egy-egy pár jelátalakító egység. Az áttekintett megoldások közül a csavart érpáras videojel továbbítás az, ami mind minőség szempontjából, mind költségvonzat szempontjából megnyugtató eredményt biztosít. Ebben az esetben a jeltovábbítás egy adó és vevő egység felhasználásával csavart érpáron keresztül valósul meg. Az adó a kamerából érkező videojelet egy előre meghatározott karakterisztikának megfelelően kiemeli, s ezáltal biztosítja, hogy a kábel okozta csillapítás ne okozzon minőségromlást a vevő által visszaalakított jelben.

8. 2. 3. *Képfeldolgozó eszközök, képdigitalizáló (grabber) kártyák*

Ahhoz, hogy a képi adat, mint digitális információ (számok sorozata) álljon rendelkezésre, egy video-digitalizáló egységre van szükség. Ez fogadja a szabványos NTSC, PAL vagy SECAM video-jelet (jeleket), és alakítja át digitális információvá a berendezés többi egysége számára. Ezek után a kép digitálisadat formájában kerül feldolgozásra, így a rendszerbe kerülő képi adat minősége és paraméterei jelentősen meghatározó tényezők a további feldolgozás szempontjából. Jelenleg a digitalizálást végző kártyák több típusa is elérhető, ám ezeknek sajnos csak a tört része hazai fejlesztésű és gyártású. Ezt a szempontot azért célszerű szem előtt tartani, mivel csupán azok a rendszerek tudnak maximális teljesítményt nyújtani, amelyiknek fejlesztői egyaránt kezükben tartják a hardvert és az erre épülő alkalmazásokat.

Napjainkban a digitális video megfigyelő rendszereknek döntő többsége IBM PC kompatíbilis számítógép alapú, melynek PCI buszába csatlakoztathatóak a grabber - kártyák. A képdigitalizáló kártyák típustól függően 3, 4 vagy 6 bemenettel rendelkeznek. A kártyánkénti bemenetek száma igen lényeges információ, hiszen ez megadja az egy számítógép felhasználásával kiépíthető rendszer maximális nagyságát. A jelenlegi IBM kompatíbilis PC-k általánosan 4-6 db PCI busszal rendelkeznek. Ami azt jelenti, hogy például egy 4 PCI busszal rendelkező számítógépet alapul véve, 4 bementtel rendelkező digitalizáló kártyákból csak 16 kamerás rendszert építhetünk maximálisan, amíg a 6 video bementtel rendelkező kártya esetében 24 kamerás rendszerek is kialakíthatóak. A bemenetek számának vizsgálatával egy időben fontos, hogy megnézzük a kártya műszaki paramétereit is, amelyek közül a rendszer működése szempontjából talán az egyik legfontosabb a kameraváltáshoz szükséges idő. A digitalizáló kártya működése ugyanis multiplexer jellegű. Megkeresi a bemenetre csatlakoztatott videojel szinkronjelét, majd miután ezt megtalálta elkészítik a megfelelő számú képmennyiséget. Ezek után átugrik a második bemenetre és újra elkezdi keresni az ott lévő videojel szinkronjelét. Az egyes kártyatípusoknál más-más időtartam (40 – 350 ms) szükséges ahhoz, hogy a digitalizáló kártya tökéletesen igazodni tudjon a kamra szinkronjeléhez. Ha például megvizsgálunk egy olyan 4 bemenettel rendelkező kártyát, amelynek a szinkronizáláshoz 300 ms-ra van szüksége, akkor világosan kiderül, hogy a kameránkénti képfrissítési idő nem lehet több mint 1,2 másodperc. Viszont egy 40 ms-os szinkronizációjú kártya esetében a kameránkénti képfrissítési idő 0, 2 másodperc, ami azt jelenti, hogy másodpercenként akár 5 kép is kapható minden egyes kameráról. A digitális video megfigyelő rendszer kiválasztásakor a fent említett paraméterek mellett fontos megvizsgálni még a következőket:

- a digitalizálás maximális felbontása (768x576 jó minőségnek felel meg)
- digitalizálási módjai: grayscale (8 bit), YUV (16 bit), RGB (24 bit)
- az alkalmazott A/D átalakító jósága (8, 10 bites)
- képes-e a kártya fekete-fehér és színes videojelek feldolgozására is
- támogatott operációs rendszerek

8. 2. 4. *Képkiértékelést, megjelenítést, tárolást végző szoftver*

A digitális video megfigyelő rendszerek felhasználókhoz legközelebbi része a képfeldolgozást és megjelenítést végző kezelőszoftver. Ezek kialakítása és jellemzői a

gyártóktól függően más és más. Általánosan elmondhatjuk azonban, hogy a szoftvereknek a következő elvárásoknak kell eleget tenniük ahhoz, hogy mind technikailag, mind biztonságilag kielégítők legyenek:

- lehetőséget kell biztosítaniuk ahhoz, hogy a felhasználók a lehető legjobban saját igényeikre tudják szabni a rendszert
- igény esetén biztosítsa az egyes kameraképek élő képes (real-time) megjelenítését (természetesen emellett a képfeldolgozásnak is működnie kell)
- gyors képfrissítés és képtárolás
- beépített mozgásérzékelő felületek (képenként több, egymástól függetlenül paraméterezhető, időkorláthoz rendelhető)
- biztosítania kell a mozgásérzékelő mellett a bizonyos feltételek melletti egyedi képtárolást
- több felhasználósnak kell lenniük (minden egyes felhasználóhoz egyedileg rendelhető jogosultságokkal)
- minden egyes kezelői beavatkozást naplóznia kell
- támogatnia kell az eltárolásra került képek exportálását (különféle szűrési feltételek mellett)
- könnyen kezelhetőnek, átláthatónak kell lennie
- támogatni kell az integrált rendszerek kialakítását
- biztosítania kell a távolról történő betekintés lehetőségét (telefonvonal, LAN, WAN, GSM)
- az alkalmazott képtömörítés jellege (beállítható legyen)
- grafikus kezelői interfésszel kell rendelkezni
- biztosítania kell az eltárolt események archiválását (DAT, HDD, DVD, CD)

8. 2. 5. *A rendszert működtető számítógép*

A digitális video megfigyelő rendszerek jelentős része IBM PC kompatibilis számítógépre épülnek. Ez az eszköz azonban eltér egy normál személyi számítógéptől, hiszen az erre háruló igénybevétel jóval nagyobb, mint például egy irodai számítógépé. Az

alkotóelemeknek egyrészt nagy megbízhatóságúaknak kell lenniük, amelyek bírják a tartós igénybevételt, másrész biztosítaniuk kell a képfeldolgozáshoz és a nagymennyiségű adat gyors tárolásához szükséges teljesítményt. A legideálisabb megoldás az, ha maga a gyártó biztosítja a digitális video megfigyelő rendszerhez a számítógépet is, így ugyanis biztosan olyan eszközöket kap a felhasználó, amelyek a megvalósítandó feladathoz a legideálisabbak (rezgésmentes kivitel, por elleni védettség, stb). Abban az esetben, ha mégis a felhasználó vagy telepítő biztosítja (megfelelő szakmai ismeretek birtokában) a működtetéshez szükséges számítógépet, mindenképpen tanácsos kikérni a gyártó véleményét, hogy milyen eszközök kerüljenek beépítésre és milyen operációs rendszerrel működik együtt a video megfigyelő rendszer.

8. 3. *Digitális video megfigyelő rendszerek integrálási lehetőségei*

Mint minden korszerű rendszertől, így a digitális video megfigyelő rendszerektől is joggal elvárható, hogy képes legyen összehangoltan működni más esetleg már előzetesen létesített rendszerekkel (pl. vagyonvédelmi-, vagy beléptető rendszer). Egy biztonsági kamera és technikai rendszer hatékonysága érdekében minden lehetséges eszközt fel kell használni a biztonság növelésére. A biztonság nemcsak technika, hanem eljárás és minőség kérdése is.

Professzionális biztonsági kamera rendszerek:

A rendszerek ötvözik a klasszikus eszközöket, mint a videó multiplexer, videó felvevő és a monitorok. Ezen kívül számos olyan szolgáltatást biztosítanak, melyek az IP alapú hálózati technológiának köszönhetőek. Ilyenek például az e-mail, sms küldés, videó anyagok tetszőleges helyre való továbbítása, vagy a távoli hozzáférés/kezelés lehetősége. A professzionális rendszerek képesek mind analóg, mind – akár többféle gyártótól származó – digitális biztonsági kameráktól érkező videó stream-eket kezelni, és az élő képeket a felhasználók felé továbbítani. Ezen felül képesek ezen videó folyamok rögzítésére eseményvezérelt, és időzített módon. Így lehetőség van az archivált felvételek hatékony kiértékelésére akár a riasztási események, akár a folyamatos felvételek között keresünk. Biztosítják az összes olyan menedzsment funkciót, mint a hagyományos rendszerek, ráadásul egyszerű kezelőfelületén keresztül sokkal hatékonyabb működést tesz lehetővé. Biztonságtechnika hálózati technológiákat (LAN, WAN, VPN, internet, vezeték nélküli megoldások, stb.) lehet használni egy nagy és kis vállalati biztonsági rendszer létrehozásához,

amely magában foglalhat lokális, helyi rendszereket és ezeket egy biztonsági rendszerbe is integrálhatja akár egy, vagy több száz biztonsági kamera alkalmazásával.

Egy standard internet böngészőn keresztül felhasználónév és jelszó azonosítás segítségével igénybe vehetők a rendszer szolgáltatásai a felhasználó geográfiai helyétől függetlenül. A felhasználó név és jelszó egyértelműen meghatározza a felhasználó jogait és lehetőségeit a rendszerben és megakadályozza azokhoz a kamerákhoz és a rendszer más szolgáltatásaihoz való hozzáférést, melyekre az nem jogosult.

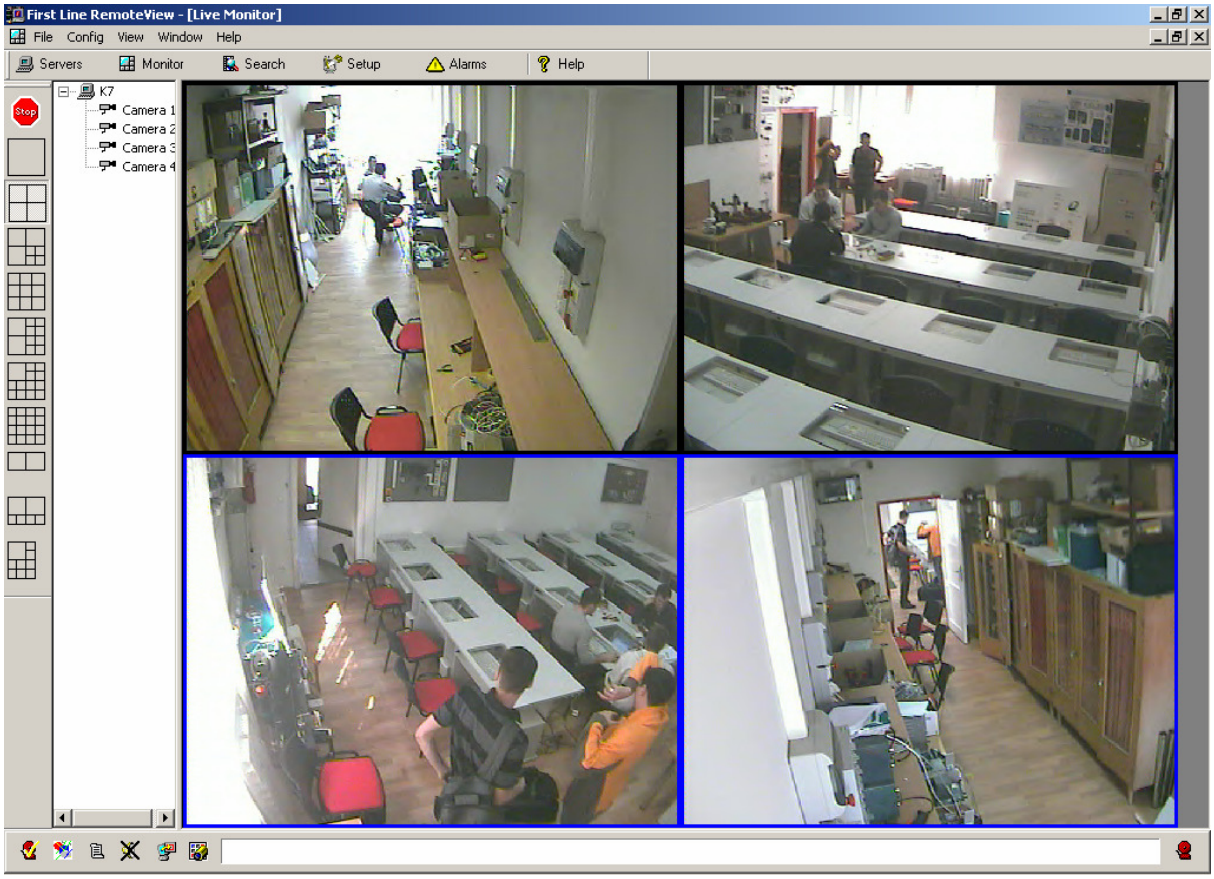
A nyílt, standard biztonsági rendszer komponensek, és interfészek használata lehetővé teszi a legköltséghatékonyabb megoldások alkalmazását a kis helyi biztonsági rendszerektől kezdve a hatalmas nagyvállalati rendszerekig. [12]

8. 4. Röviden a CyberStation kamerarendszeréről:

Ez egy PC alapú rendszer, mely biztonságos, rugalmas, és könnyen kezelhető, a laikus felhasználó számára is. Nagyszerű tulajdonsága, hogy az interneten keresztül, az arra jogosultak a telephelyen kívül is bármikor szemmel tarthatják értékeiket, valamint telefonhívás kezdeményezésére is képes a rendszer, vagy E-mailt küld a megadott címekre a mozgások érzékelésének pontos helyéről és idejéről, ha ezeket a funkciókat a felhasználó igényli.

A csomag egy szerver, és egy kliens programból áll. A szervernek viszonylag nagy a kapacitás igénye, azon kívül másra nem használható a számítógép, legfeljebb néhány hasonló elven működő vagyonvédelmi program futtatható rajta. Esetünkben a CyberStation beléptető rendszere működik párhuzamosan a szervergépen is. A kliens része viszont teljesen észrevétlen, ha nincs használatban. Hatalmas megtakarítást jelenthet ez, ha több helyről óhajtja a felhasználó szemmel tartani a rendszert. Nem kell külön monitorokra vezetni a kamerák képeit, elég egy már meglévő helyi számítógépes hálózatra csatlakoztatni.

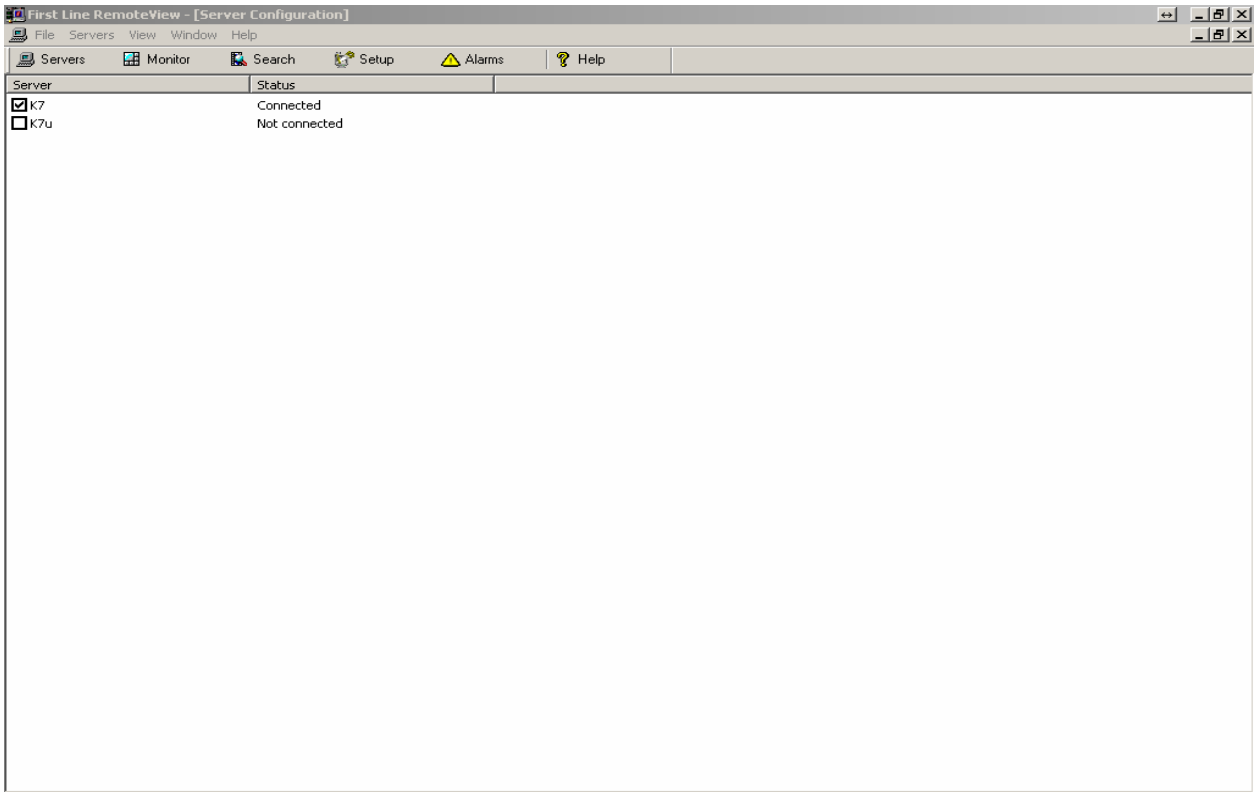
A dolgozatomban tárgyalt és kiépített beléptető rendszerhez felszerelésre került 4 analóg DSP kamera. Ezeket a video eszközöket a Continuum Cyberstatation programja vezérli és a kamerák képeit egy a K/7- s labor tanári gépén futtatható First line Remoteview alkalmazással érhetjük el. A First line Remoteview indítása után alapesetben következő képernyő fogad minket:



24. ábra: Pillanatkép a labor kamerarendszeréből

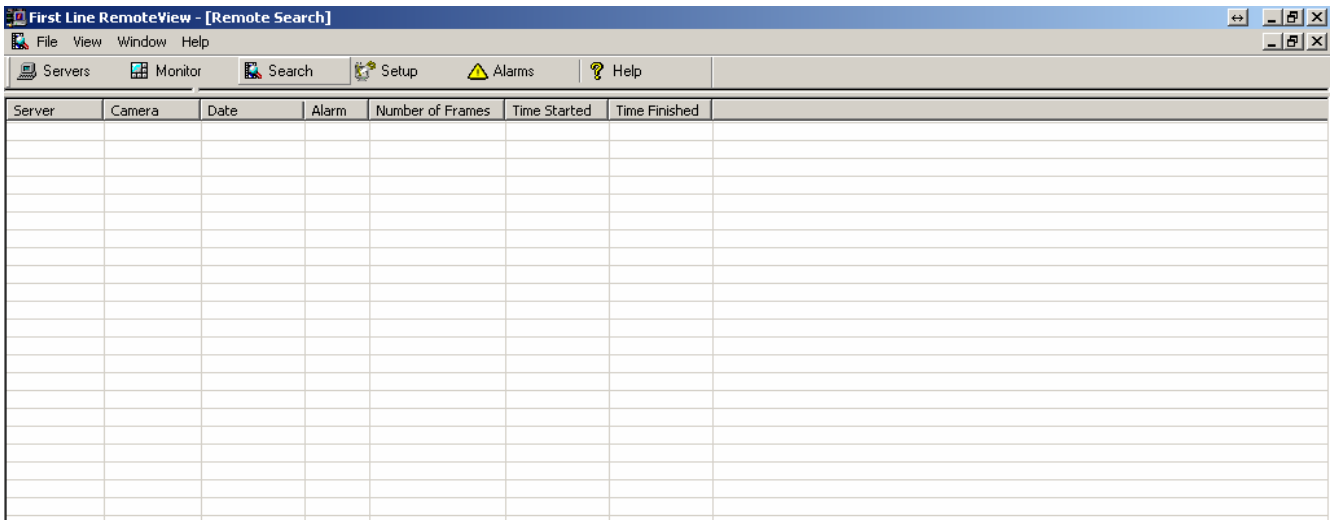
Az alkalmazás valósidejű képet ad a teremről és a bal oldali menüből látszik, hogy a négy felszerelt kamerát külön - külön is megtekinthetjük.

A programból információt kaphatunk a csatlakozott szerverek számáról, ha a server menüpotra kattintunk.



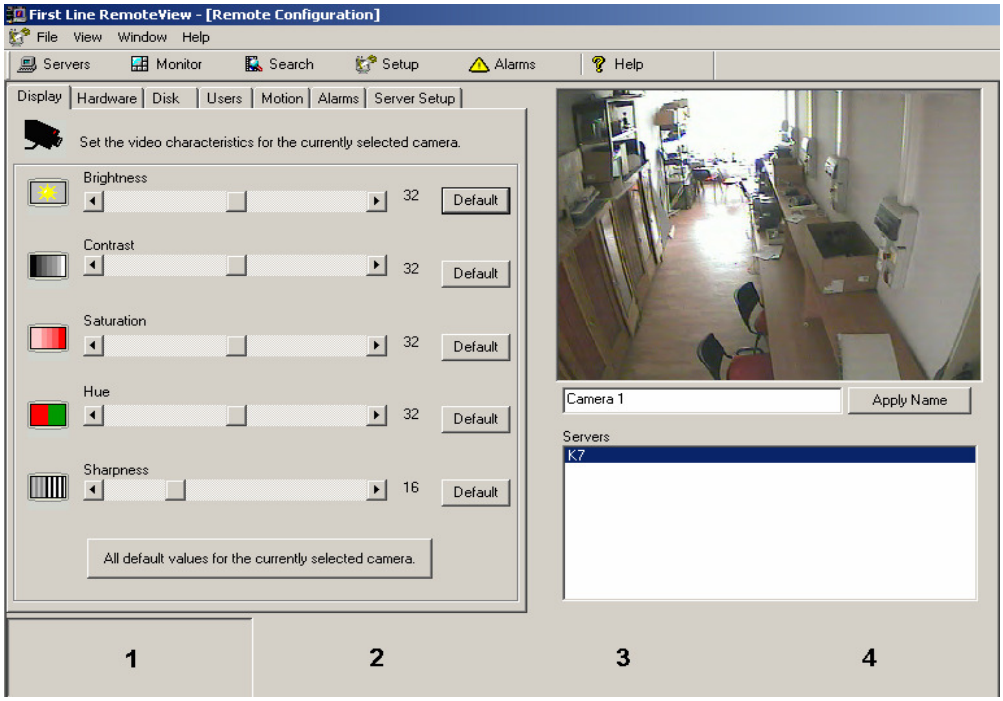
25. ábra: Szerverek csatlakozásáról megjelenítendő információk

A search funkció lehetővé teszi számunkra a riasztások közötti kereséseket. Kereshetünk, server-, a kamera száma, az eltárolás dátuma alapján vagy akár időintervallumot is adhatunk, meg amely közötti adatokat kívánjuk megtekinteni.

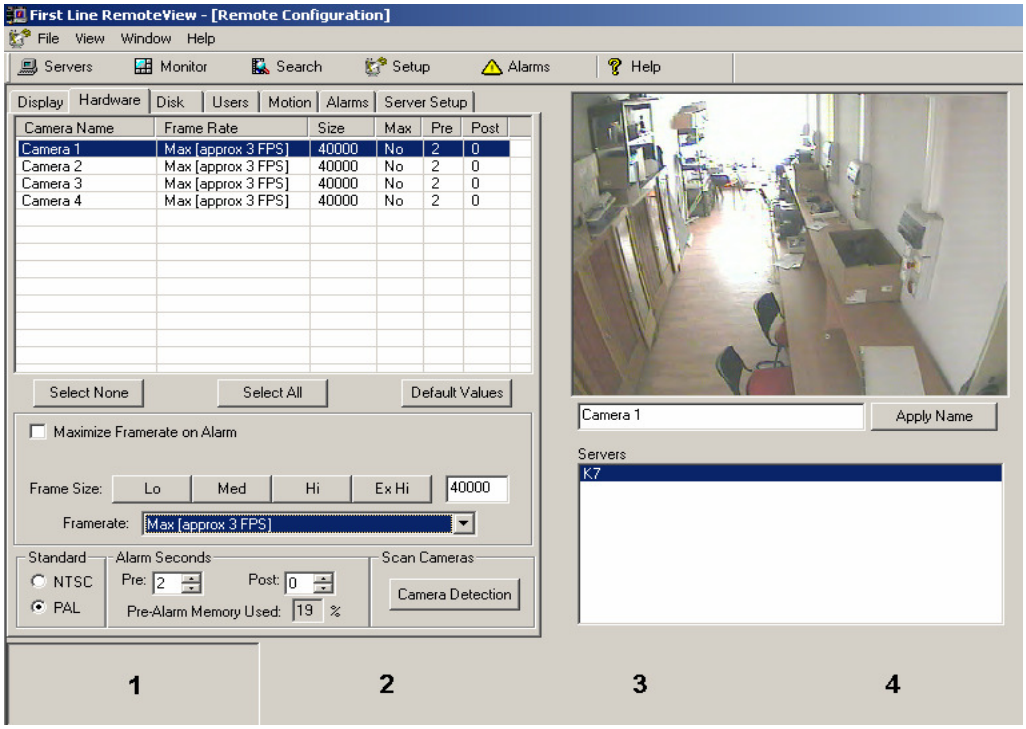


26. ábra: Keresés az eltárolt adatok között

A kamera beállításait a setup menüpontban testre szabhatjuk:



27. ábra: Kamera beállításainak opciói

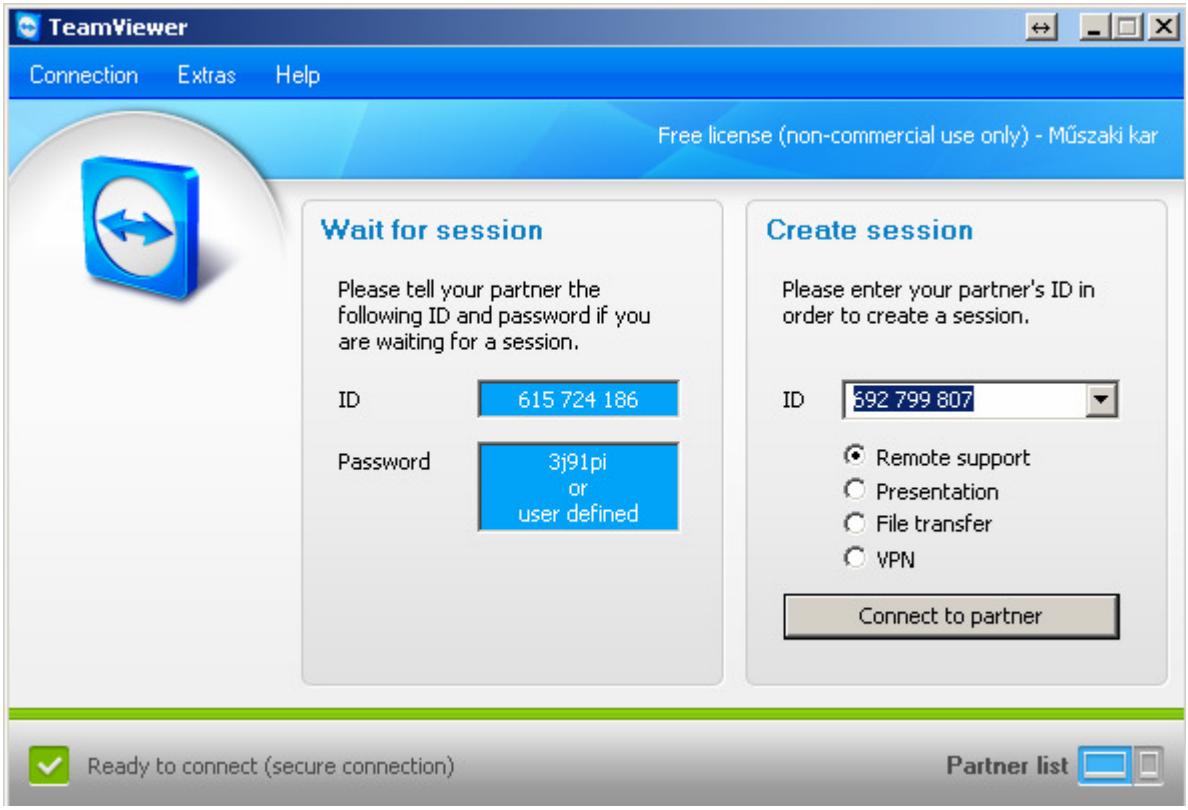


28. ábra: Kamera display beállításai

Akár külön-külön is változtathatjuk a kamerák beállításait, a kamerák közötti váltást az alsó sorban elhelyezkedő 1-2-3-4 számok teszik lehetővé. A 27. és 28. ábrákon a rendszerünkhöz alkalmazott kijelző és kamera beállításokat tekinthetjük meg.

8. 5. Távoli elérés megvalósítása

A távoli elérését a K/7- s teremben levő gépnek egy ingyenes szoftver segítségével oldottuk meg. A szoftvert (ha ezt az opciót választjuk) még installálnunk sem kell, egyszerűen elindítjuk, és máris működik. Ez az opció nagyon hasznos, ha publikus helyekről szeretnénk hozzáférni egy másik számítógéphez. A dolog működésének egyetlen (fontos) feltétele van: a teamviewer - nek futnia kell azon a gépen is, amelyiket irányítani akarjuk. Ha mindkét gépen fut a szoftver, beírjuk távoli gép azonosítóját, azaz ID - jét. (a gépek ID-jét a szoftver elindítása után kijelzi).



29. ábra: Teamviewer indulásakor beállítandó adatok

Csatlakozás előtt számos lehetőség közül választhatunk: van csak fájlmegosztás (másolás, törlés és megnyitás), de van „prezentációs” mód is: ekkor teljes vezérlést kapunk a távoli gép munkaasztalához, mintha csak a saját PC-nk előtt ülnénk. Ezen felül választhatjuk a rendszergazdák által jól ismert VPN módot is. A fájlátvitel a legkönnyebben használható szolgáltatás: gyakorlatilag olyan, mint egy FTP, vagy bármilyen fájlkezelő. A prezentációs

mód már jóval izgalmasabb és több mindenre is használható. Ebben az esetben (persze, csak ha a távoli gépen is engedélyezve van), akár teljes hozzáférést is kaphatunk a távirányított számítógéphez, programokat és rendszerablakokat nyithatunk meg és használhatunk – az apró sebesség különbséget leszámítva (hiszen távoli eléréssel minden egy kicsit lassabban reagál) teljesen olyan mintha ott ülnénk a szóban forgó PC előtt. A szoftver a biztonságra is ügyel: a hozzáféréseket csoportokba rendezhetjük, biztonsági szint szerint, így pontosan megadhatjuk, hogy kik- honnan, és milyen mélységig férhetnek hozzá a a szervergéphez.

A Teamviewer működik tűzfalakon keresztül is, sőt a kapcsolat nincs két felhasználóra korlátozva, akár több személy is hozzáférhet ugyanahhoz a géphez. A biztonságért az ún. RC4 session kódolás felelős, amely minden adatot kódolva küld el a hálózaton keresztül, ez RC4 a szabvány SSL protokollra épül, tehát elég biztonságos, és persze minden hozzáférés (és próbálkozás) logolva van. [13]

9. Összegzés

Szakdolgozatomban az IAS automatika által szerelt TAC eszközök mellett más gyártók terepi eszközeit felhasználva egy informatikai labor beléptető rendszerének megvalósításával és elemzésével foglalkoztam. Célom az volt, hogy egy olyan működőképes rendszer alakuljon ki, amely megfelel a mai kor követelményeinek és költséghatékony is.

A rendszerrel szemben támasztott követelmények a következők voltak: legyen biztonságos, naplózza a belépési eseményeket, és könnyen menedzselhető adatbázissal rendelkezzen. A tervezés felhasználó szemléletmódban történt, nagy figyelmet fordítottam a könnyű kezelhetőségre.

A rendszer a felhasználók azonosítására proximity kártyákat és olvasót használ. A felhasználók adatai egy adatbázisban, egy központi szerveren kerülnek tárolásra, a beléptető-pontok ezt a közös adatbázist használják az azonosításhoz. A szerver és a beléptető pontok Ethernet hálózaton keresztül TCP/IP protokollcsalád segítségével kommunikálnak egymással. Tehát nem szükséges, hogy a szerver és a beléptető pont egy helyen legyenek, mivel a rendszerhez az interneten keresztül számos további beléptető pont csatlakoztatható.

A laborban felszerelésre került analóg mozgásérzékelőkkel ellátott kamerák teljes körűen felügyelik a helyiséget, működésbe lépésükkor tárolják az adatokat. Terveink szerint egy olyan rendszert szerettünk volna létrehozni, amely nyomon követhetővé és felügyelhetővé teszi a laborba történő belépéseket és az ott folyó munkálatokat.

Célunk megvalósult, a rendszer jelenleg a Debreceni Egyetem Műszaki Karának laborjában üzemel, továbbfejlesztése az egyre magasabb szintű felhasználói igények kielégítése érdekében folyamatban van.

Irodalomjegyzék

[1] Dr. Bánhidi László: Épületgépészet a gyakorlatban 1.,2.,3. kötet

22-26p. és 111-116p.

[2] http://www.hambell.hu/content/show/reszletes_leiras

letöltve: 2010.04.13.

[3] Faragó László: A jövőalkotás társadalomtechnikája. Dialog Campus kiadó, 2005. 172-178 p.

[4] http://www.hambell.hu/content/show/reszletes_leiras

letöltés 2010.04.17

[5] TAC Andover Continuum katalógus, 2007.

[6]http://www.riasztobolt.hu/pictures/b/nagykep_kamera_cnbg1862.gif&imgrefurl=http://www.riasztobolt.hu/product/webaruhaz/1688/CCTV---VIDEOS-ESZKOZOK-Kamerak-es-reszegysegeik-Kamerak-day---night-normal-Valos-day---night/CNB-G1818PF.html%3FIMRSID%3Dtu8o1454tg20mud7ofuslu0uf0&usg=__sVqbcWSfRHkG5LoQAXvGLec7abA=&h=400&w=400&sz=32&hl=hu&start=2&um=1&itbs=1&tbnid=hCD4JgAzqIXVsM:&tbnh=124&tbnw=124&prev=/images%3Fq%3Dcnb%2Bkamer%25C3%25A1k%26um%3D1%26hl%3Dhu%26sa%3DN%26tbs%3Disch:1

[7] http://www.hpnrgate.hu/kartyak.htm

letöltve 2010.05.02

[8] http://www.hpnrgate.hu/kartyak.htm

letöltve 2010.05.02

[9] http://www.kilowatt.hu/termekkep/C60N.htm

letöltve 2010.05.05

[10] Dr. Szandtner Károly, Dr. Kovács Károly – Épületinformatika, Budapest 2002.

[11] www.thermocontrol.ro/TAC_szabalyzok_szoftver_brosura.pdf

letöltve 2010.05.06

[12] Kondor Tamás – Video megfigyelő rendszerek, Budapest kiadó, 2003.

[13] http://www.teamviewer.com/download/version_4x/teamviewer_manual.pdf

letöltve 2010.05.

Köszönetnyilvánítás

Köszönetemet és mélységes tiszteletemet szeretném kifejezni Bartha István Tanár Úrnak, aki elvállalta szakdolgozatom témavezetését, valamint a közös munka során segítőkészségéről, rugalmasságról, hozzáértéséről tett tanúbizonyságot. Hálás vagyok, hogy hozzájárult ahhoz, hogy elmélyedhessek az épületinfomatikai rendszer

feltérképezésében, valamint hogy lehetőséget és alkalmat biztosított a rendszer széleskörű megvalósításához és megismeréséhez.

Továbbá szeretném megköszönni az IAS automatika szakembereinek, akik a rendszer kiépítése után rendelkezésemre bocsátották az elemzéshez szükséges kézikönyveket és egyéb segédanyagokat.

Nem utolsó sorban köszönetemet fejezem ki a Debreceni Egyetem könyvtári dolgozóinak, akik az adatgyűjtés során maximálisan segítették munkámat.