BÁNKI KÖZLEMÉNYEK
1. ÉVFOLYAM 3. SZÁM

Elektronikus vagyonvédelmi rendszerek lehetséges kiegészítő funkciói

Possible additional features of electronic property protection systems

Beszédes Bertalan
Óbudai Egyetem, Alba Regia Műszaki Kar, Székesfehérvár, Magyarország
beszedes.bertalan@amk.uni-obuda.hu

***Összefoglalás* — A cikk a komplex vagyonvédelmi rendszereknek, azok elektronikai védelmet megvalósító komponenseivel foglalkozik. Ezen belül kiemelten az elektronikus kültéri védelem, a behatolást jelző rendszer és a beléptető rendszer lehetséges kiegészítő funkcióinak ismertetésével. A bemutatott megoldások hardverigény tekintetében törekszenek a rendszer költségeinek alacsonyan tartására, valamint a szoftveres lehetőségek kihasználására.**

***Kulcsszavak*:** elektronikus vagyonvédelmi rendszer, kültéri védelem, behatolás-jelző rendszer, radar szenzor, ultrahangos távolságmérő, jelenlét érzékelés, rezgésérzékelő, piezoelektromos szenzor, gyorsulás érzékelő, beléptetőrendszer, személyazonosítás.

***Abstract* — The article deals with the electronic protection component, within the complex property protection systems. In particular, it describes the possible complementary functions of electronic outdoor protection, the intrusion detection system and the access control system. The solutions presented here is aimed to keeping the system's hardware costs low, and to use software opportunities.**

***Keywords*:** electronic property protection system, outdoor protection, intrusion detection system, radar sensor, ultrasonic distance meter, presence detection, vibration sensor, piezoelectric sensor, acceleration sensor, access control system, personal identification.

1 BEVEZETÉS

Az elektronikai védelem feladata a behatolás, behatolási szándék érzékelése és értesítés küldése az élőerős védelem számára. Az élőerős védelem helyszínre vonulásának és megfelelő reagálásának következtében a vagyon elleni támadás elhárítható. [1]

A rendszerben kritikus tényező az idő. Ha az élőerős védelemnek nincs lehetősége a jogellenes behatolás és távozás időtartalma alatt a helyszínre érni és intézkedni, a behatoló elmenekülhet az esetleges-en megszerzett javakkal. Az elektronikai védelem képes a behatolást jelezni, mielőtt a behatoló a védett épületen, épületrészen belül kerülne – így megnövelve a reagálásra fordítható időt. Ebben az esetben a rendszernek elengedhetetlen összetevője – a védendő értéktől függően – a megfelelő szintű mechanikai védelem, amelynek célja a behatolás akadályozása, behatolásra fordítandó idő kitolása.

2 ELEKTRONIKUS VAGYONVÉDELMI RENDSZER FELÉPÍTÉSE

Az elektronikus kültéri védelmi és behatolás-jelző rendszerek egy központi egységből, legalább egy érzékelőből és kiépítéstől függően egy vagy több beavatkozó és/vagy értesítő egységből épülnek fel.

A központi egység fő feladata a riasztórendszer vezérlése, a különböző egységei közötti kommunikáció biztosítása, a beérkező adatok értelmezése, és a beavatkozásra képes egységek vezérlése. Kültéri védelemi és behatolást jelző rendszerek feladata a védett területre történő behatolás érzékelése. A beavatkozó egység célja a behatolóval szembeni fellépés, az értesítő egységé pedig értesítés küldése az élőerős védelemnek.

2.1 Eszközök közötti kommunikáció

A részegységek közötti kommunikáció történhet vezetékes vagy vezeték nélküli összeköttetésen. Az egységek a megfelelő eszközökkel zavarhatók, tönkretehetők, ezért célszerű megfelelő árnyékolással ellátni ezeket. A vezetékezés is alkalmas a zavar felvételére és az egységekbe történő bejuttatására. Célszerű árnyékolt vezetékezést használni (akár kétszeresen árnyékolt kábelt), valamint a vezetékeket zárt csőhálózatba telepíteni. Az ilyen kialakításnál, a csőcsatlakozásokkal szemben elvárás a csőszakaszok közötti jó galvanikus kontaktus biztosítása, illetve az elektromágneses hullámokkal szembeni jó csillapítóképesség. A kiterjedt fémhálózatot mind zavarvédelmi, mind életvédelmi szempontból csatlakoztatni kell az egyenpotenciálra hozó hálózattal. A fenti kiépítés nagyban megnöveli a telepítés anyag- valamint munkadíj-költségét is, csak indokolt esetben célszerű alkalmazni.

A vezeték nélküli összeköttetés mentesíti a felhasználót a vezetékezés költségeitől – különösen utólagos telepítés esetében. A vezetéknélküli érzékelő anyagköltsége viszont magasabb a vezetékes, hasonló paraméterű érzékelőénél. Az optimális megoldás sok esetben egy hibrid rendszer kiépítése. Lehetőségként kínálkozik a behatolók számára a vezetéknélküli egységek jeleinek elnyomása, helyettesítése, így az említett megoldás kisebb biztonsági szintet eredményez. Megoldásként kínálkozik a vezetékhálózaton érkező, valamint elektromágneses sugárzás formájában megjelenő zavaró jelek érzékelése, kiegészítő érzékelő segítségével. Amennyiben a zavarjel vagy zavarsugárzás meghalad egy előre meghatározott

szintet, az alrendszer jelzést küld a központnak, amit az szabotázsként érzékel [2].

Célszerű egy külső szerverrel is lekérdezni (a szerver felé jelenteni) a központ működőképességét. Amennyiben a központ nem ad életjelet vagy hibakódot küld, a szerver értesíti az élőerős védelmet. A behatolónak lehetősége nyílhat beépülni a kommunikációs csatornába, így elfedni, meghamisítani az üzenetváltást. Amennyiben alkalmazott ez a megoldás, lehetőség van egy, a központnál elhelyezett, fizikailag védett, galvanikusan leválasztott, csak egyirányú adatforgalmat megengedő, írható adattároló telepítésére. A központ az említett másodlagos háttértárolóra archiválhatja a kiküldött és vett üzeneteket. Amennyiben a külső szerveren tárolt adatok és a másodlagos háttértárolón tárolt adatok nem egyeznek meg, szabotázs történt [2]. Az élőerős védelem feladata az adatok összehasonlítása.

Az élőerős védelem értesítése hagyományosan történhet számítógéphálózati eszközökön keresztül vagy GSM hálózaton keresztül. Kínálkozik egy eddig még nem alkalmazott alternatív csatorna is a kis adatmennyiség átvitelére. A Narrow Band-IoT egy szabványosított, LTE infrastruktúrán használható mobil technológia, alkalmas kis adatmennyiségek átvitelére. A meglévő mobilhálózatot használja, ezzel biztosítva van a jó lefedettség, licens-elt (1-2€ / év eszközönként), azaz a szolgáltató garantálja a minimális sávszélességet és a hálózathoz való hozzáférést. Célszerű több csatorna egyidejű használata az élőerős védelemmel történő kommunikáció során.

A központi egység is tartalmaz akkumulátoros tartalék-áramforrást. Lehetőség van a szigetüzemű tápellátásoknál is alkalmazott megoldások telepítésére is [3]. Fontos, hogy a rendszer fel legyen készítve az ilyen irányú támadások elhárítására is, például a napelemek vezetékein keresztüli zavarás, túlfeszültség érzékelésére, levezetésére. Indokolt esetben kiépíthető redundáns tápellátási rendszer is [4]. Az említett megoldás szintén jelentősen növeli a telepítés költségeit.

2.2 Kültéri védelem és behatolást jelző rendszerek

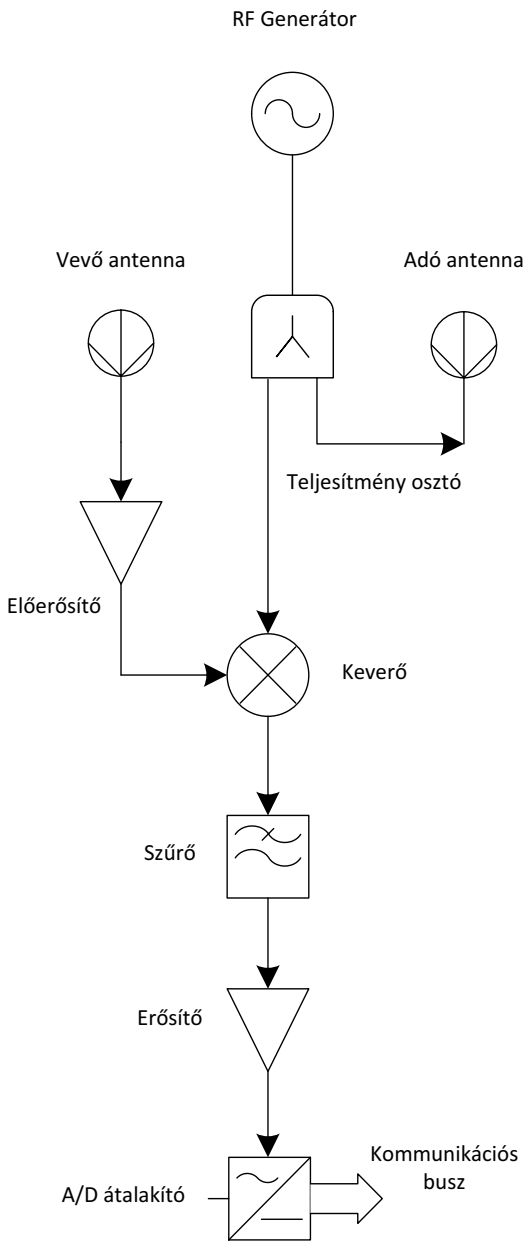
A behatolás érzékelésére és a behatoló tevékenységének nyomon követése érdekében védelmi köröket kell létrehozni. A fentieket a kültéri védelem, a felületvédelem vagy héjvédelem, az épületen belüli térvédelem, és a tárgyvédelem eszközeivel biztosíthatjuk. [1]

Mozgás- és/vagy jelenlétérzékelésre a gyakran alkalmazott lépésjelzők, a mágneses térérzékelők, infrasugaras eszközök, mikrohullámú eszközök, passzív infraérzékelők, rezgésérzékelők mellet lehetőség van videó megfigyelő rendszerek telepítésére is.

Cél a költséghatékony kiegészítő lehetőségek bemutatása, ezért a továbbiakban elsősorban az alacsony költségű radar szenzorok, ultrahangos távolságmérők, és rezgésérzékelők ismertetése és alkalmazási lehetőségei következnek.

2.2.1 Radar szenzorok

A radar szenzorok egy adó és egy vevő egységből állnak, felépítésük blokkdiagramja az 1. ábrán látható. Felhasználásukkal, egy objektumról visszaverődött jel feldolgozásával nyerhető információ. A Doppler effektus kihasználásával [5] nem csak a szenzortól való távolság mérésére, hanem az objektum sebessége is megállapítható, a visszavert hullám frekvenciájának változásából – jellemzően nx10Hz (2. ábra). (A sebességadat a szenzor szempontjából vizsgálva igaz.) Az üveget leszámítva minden általános építőanyagon keresztülhatolva képesek érzékelni a jelenlétet, így fa, műanyag vagy gipszkarton burkolat mögé, vakolattal vagy tapétával fedett kötődobozba is elhelyezhetők.

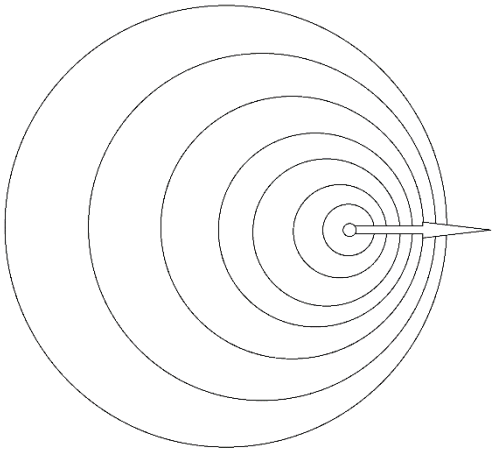


1. ábra: Radar szenzor általános blokkdiagramja

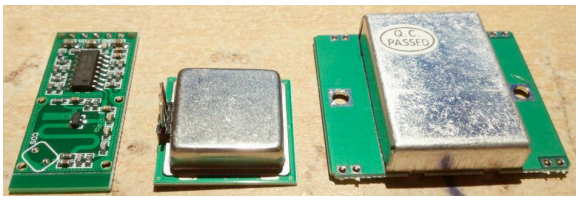
A különböző típusú, polgári célokra kiépített riasztórendszerek kiegészítésére használható, költséghatékonyan beszerezhető modulok a 3. ábrán láthatók, a hozzájuk tartozó főbb tulajdonságok az 1. táblázatban vannak összegezve. A baloldali típus, az elvégzett kísérletek alapján inkább csak jelenlét érzékelésre, távolság mérésére alkalmas, a másik két típus az említetteken felül alkalmas sebesség mérésére is.

A bemutatott radar szenzorok felhasználhatók a kültéri védelem területén, például: épület megközelítése, épület vagy oszlop melletti elhaladás, ajtó megközelítésének

érzékelésére. Valamint jól használhatók térvédelem eszközeiként, például: folyosón történő haladás, ajtó megközelítésének érzékelésére.



2. ábra: Doppler-effektus



3. ábra: Radarszenzorok: RCWL-0516, PD-V11, HB100

1. táblázat: Radar szenzorok jellemzőinek összehasonlítása

	RCWL-0516	PD-V11	HB100
Árfekvése	500 HUF	1300 HUF	1500 HUF
Érzékelési szögtartomány	360°	180°	180°
Működési frekvencia	3.181 GHz	24.125 GHz	10.525 GHz

2.2.2 Ultrahangos távolságérzékelők

Az ultrahangos távolságérzékelők működési elve a mikrohullámú radar szenzorokhoz hasonló. Ebben az esetben is egy adó és egy vevő modul szükséges az érzékeléshez. Az adóból induló jelsorozat egy – méréshatáron belüli – objektumról történő visszaverődés segítségével jut el a vevőbe, a jelkibocsátás és a jelfogadás közötti időkülönbségből becsülhető az objektum és a szenzor távolsága.

A hang levegőben történő terjedési sebessége függ a hőmérséklettől és a páratartalomtól. Ezen paraméterek mérése nélkül is jól alkalmazható a szenzor jelenlét érzékelésére és távolság becslésére, de pontos távolságméréshez szükség van a légtér tulajdonságainak vizsgálatára. A hőmérséklet és páratartalom mérése elvégezhető kisértékű szenzorok segítségével, a korrigált távolság az alábbi kifejezés segítségével adható meg:

$$d = (v_0 + 0{,}606*T + 0{,}0124*H)*t / 2 \qquad (1)$$

ahol v0=331,39m/s, az ultrahang sebessége száraz közegben, 0°C-on, T a hőmérséklet Celsius fokban, H pedig a páratartalom.

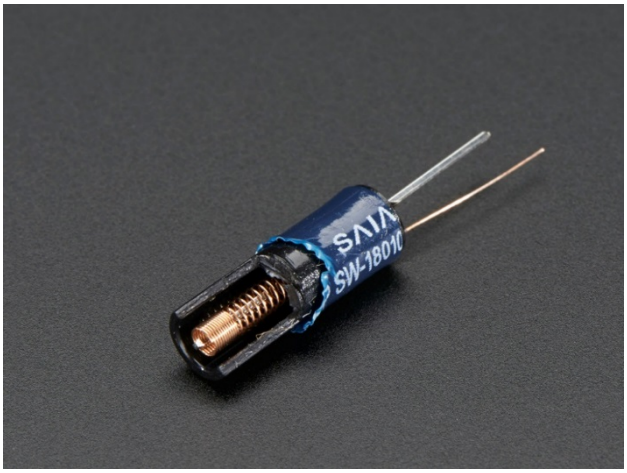
Fontos megjegyezni, hogy az ultrahangos távolságérzékelők beltérben alkalmazhatóak. A légmozgás könnyen eltérítheti az ultrahang-hullámokat, ezzel elkerülve a vevő modult, így hibás mérést eredményezve.

Térvédelemre viszont jól használhatók az egy modulban elhelyezkedő adó és vevő egységek, valamint a fizikailag különválasztott adó- valamint vevő egység pár is. Utóbbi esetben lehetőség van egy üzemidőben változó tér mozgásra történő biztosítására. A riasztórendszer élesítésekor – egy statikus helyzetben – a hanghullámok az adóból kiindulva, csillapítva és visszaverődésekkel együtt érkeznek meg a vevőbe. A beérkező mintát az alrendszer tárolja, ehhez hasonlítja a később érkező mintákat. Ha a biztosított térben van olyan objektum, ami helyet vagy alakot változtat, akkor a hanghullámok csillapítása, visszaverődései megváltoznak. A megváltozott jel el fog térni az élesítéskor mintavételezett referencia jeltől, ami központba küldött riasztást kiváltó jel indítását fogja eredményezni. Az aktuális referenciamintától való megengedett eltéréssel befolyásolható az alrendszer érzékenysége.

Lehetőség van az ultrahangos szenzor radarszenzorral és PIR szenzorral való kombinált használatra a megbízhatóbb térvédelem kialakításának érdekében.

2.2.3 Rezgésérzékelők

Az alábbi alacsony anyagköltségű rezgésérzékelők jól használhatók a héjvédelem eszközeiként (4. ábra). A záródó kontaktus vagy a rezgés mintázata is információtartalommal bír az őt felügyelő alrendszer számára. A rugós rezgésérzékelők geometriai és anyagtulajdonságoktól függően változó karakterisztikákkal szerezhetők be. Kialakítástól függően választható alacsonyabb, illetve magasabb frekvenciákra érzékenyebb szenzormodulok, valamint a – például: ajtóra történő – rögzítés módjával is befolyásolható az érzékenység.



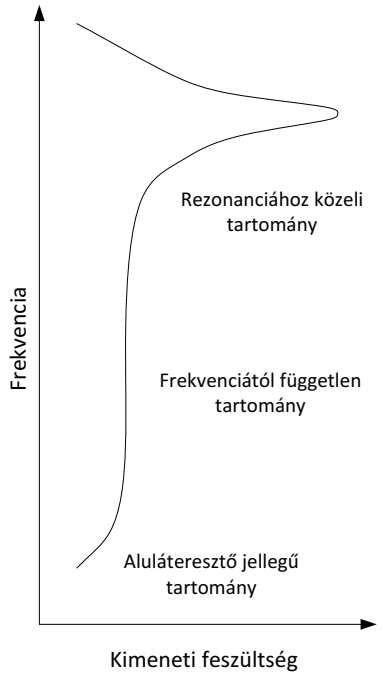
4. ábra: Rezgésérzékelő szenzor [8]

<u>Piezoelektromos szenzorok</u>

A piezoelektromosság olyan fizikai jelenség, melynél erőhatás következtében elektromos polarizáció (töltésszétválasztás) lép fel, így egyszerűen megvalósítható a mechanikai erőhatás – feszültség konverzió.

A magasabb frekvenciájú rezgésekre reagál [9] nagyobb kimeneti feszültséggel a szenzortípus (5. ábra). A széles

felhasználási lehetőségekből a héjvédelem és tárgyvédelem eszközeit kiemelve, jól és költséghatékonyan használhatóak, rezgések és vibrációk detektálására (6. ábra).

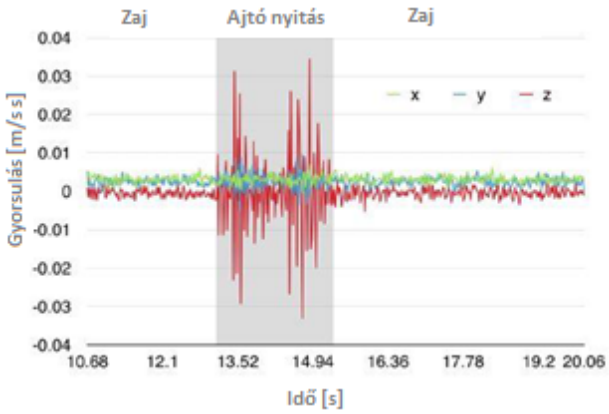


5. ábra: A piezoelektromos szenzor konstans amplitúdójú erőhatás hatására leadott a kimenetén megjelenő feszültség a frekvencia függvényében

6. ábra: Piezoelektromos érzékelő

MEMS modulok

Két és három tengelyes gyorsulásmérő szenzorok alacsony költségráfordítással beszerezhetők. Sok szenzor a tengelyek körüli elfordulás mérésére is képes. A szenzorokban elhelyezett, erőhatás bekövetkezésekor elmozdulni képes tömeg – a kondenzátor egyik fegyverzete – segítségével, a kapacitás-mérés elvére visszavezetve megállapíthatók a szenzort érő gyorsulás és elfordulás-értékek. Jól használhatók a tárgyvédelem és a héjvédelem területein, például: mozgatás, üvegtörés, ajtónyitás, fúrás, feszítés rezgéseinek érzékelésére. A szenzor jeleit feldolgozó alrendszer a mért értékek alapján képes megkülönböztetni a behatolásra jellemző jelalakot [10], például a szomszéd lakásban becsapott ajtó jelalakjától (7. ábra).



7. ábra: Mért gyorsulási értékek egy ajtónyitási próbánál

2.2.4 Fizikai jellemzők megváltozása

Héjvédelem esetében jól használhatók kiegészítő szenzorként behatolás detektálására a belső teret vizsgáló eszközök. A léghőmérséklet, páratartalom, légnyomás [11], széndioxid-szint, fényerő mért értékeinek lokális, nagy meredekségű megváltozása jelenthet egy ajtó- vagy ablak nyitást. Biztosabb a kiértékelés az épületen kívüli tér fizikai tulajdonságainak ismeretében.

Fontos a kiértékelést megzavaró tényezők figyelembe vétele a szenzorok elhelyezésekor, például: az ablakon bejutó napsugárzás fény és hőhatása, valamint a téves riasztásra okot adó események szinkronizálása az alrendszerrel, például: automatikus szellőztető vagy fűtő/hűtő berendezések használata. A jól felkészített belső tér monitorozó alrendszer jelzést kap a riasztórendszer részét nem képező belső tér tulajdonságait befolyásoló egységek működéséről, ez alapján módosítani tudja a megváltozott fizikai paraméterek által kiváltott szabotázs-jelzések súlyozását. A fenti alrendszer alacsony anyagi ráfordítást igényel, de jelentősen növelheti az elektronikus vagyonvédelmi rendszer megbízhatóságát.

2.3 Beléptető rendszerek

A beléptető rendszer feladata a védelmi körök határain – valamint az egy védelmi körön belül kialakított szakaszok határain –, átlépésére használható pontokon való átjutás szabályozása, a felhasználók jogosultságainak ellenőrzése, a felhasználók azonosítása, és a felhasználók áthaladásának szabályozása. A beléptetőrendszer kapcsolatot tart az elektronikus vagyonvédelmi rendszer központi egységével, illetve vezérli a szakaszhatárra telepített áthaladást engedélyező vagy tiltó beavatkozó egységet. [1]

2.3.1 Személyazonosítás

A dolgozat a személyazonosítás lehetséges módjaira tér ki részletesebben, továbbra is célul kitűzve a költséghatékony megvalósítási lehetőségek ismertetését. A személyek azonosítására szolgálóinformáció három csoportba sorolható be. Ezek a tudás alapú, a birtok alapú, és a biometrikus azonosítás.

Tudás alapú azonosítás

Tudás alapú azonosítás esetében a felhasználó a saját, titkos jelszavát adja meg a kezelőn. Jelszóegyezés esetében a kezelő engedélyezi az elektronikus vagy elektromechanikus beléptető egység működését. A leggyakrabban alkalmazott felhasználói felület a nyomógombokkal vagy érintő felületen kialakított billentyűzet. Egy újszerű koncepció a forgó jeladó(k), végállással rendelkező elfordulás mérő(k), toló kapcsolók felhasználói jelszóbeviteli lehetőségkét történő alkalmazása. A megszokottól eltérő kivitel nehezítheti a behatolást.

Kulcs vagy birtok alapú azonosítás

Célszerű a belépő személyének azonosítását is elvégezni a jelszó validálása mellett, így biztosítva a különböző felhasználókhoz tartozó jogosultsági szinteket, valamint a módszer felhasználásával naplózható a felhasználók tevékenysége is. Ezt nevezik kulcs vagy birtok alapú azonosításnak. Kiküszöbölhető az illetéktelen behatolás abban az esetben, ha a behatoló ismeri a felhasználói azonosító-jelszó párost és a belépésre jogosult felhasználó a rendszer által felügyelt területen belül helyezkedik el. Kiküszöbölhető, egy felhasználó kétszeri belépése ugyanarra a területre, illetve az egy felhasználó több különböző területen történő egyidejű jelenléte.

További megszorítások alkalmazásával a biztonsági szint növelhető, például: az egymástól beléptető rendszerrel elválasztott területek között csak a megengedett átjárókon keresztüli közlekedéssel, vagy riasztást generálva egy vagy több terület kihagyásakor, az utolsó kilépési ponttól fizikailag távoli belépést megkísérlő érvényes felhasználói azonosító-jelszó páros használatakor, vagy a felhasználó a területről történő kilépését követő és egy másik szomszédos területre történő belépési kísérlet között eltelt, az engedélyezettnél rövidebb vagy hosszabb időtartam esetében. Az említett lehetőségek feltétele a különböző beléptető rendszerek rendszerbe kötése, a központtal való kommunikáció biztosítása. A belépések darabszámának korlátozása is lehetséges egy adott területen -, egy adott időtartományon belül. Az időnként előforduló kivétel engedélyezése egy magasabb prioritási szinttel rendelkező személy számára elérhetővé tehető.

A fizikai kulcs lehet passzív, aktív vagy intelligens eszköz, az utóbbi a legmegbízhatóbb, beépített műveletvégző képességének köszönhetően. A megvalósított modell jelenlegi állapotában egy aktív RFID olvasóval képes a felhasználók megkülönböztetésére.

A beléptető rendszert fizikai valójukban, kezelő telepítési helyén jelen lévő személyek használják. Érdemes a kezelőnél elhelyezett szenzorral elvégezni a jelenlét érzékelését, az illetéktelen távoli engedélyezés kiküszöbölésének érdekében.

Radar szenzorok felhasználásával és további szoftveres kiegészítéssel, különbség tehető lassú, átlagos tartományon belüli és gyors mozgás között, például: előszobában elhelyezett beléptető kezelőfelület esetén, előírhatunk a megközelítésre vonatkozó mozgási szabályokat időtartamokhoz kötve.

Biometrikus azonosítás

A megszerezhető kulcs vagy jelszó nélküli, megbízható azonosítás nyújtja a legmagasabb biztonsági szintet de egyben ez a legköltségesebb megoldás is a megvalósításhoz igényelt hardver- és szoftvereszközök felhasználása miatt.

Továbbra is cél a költséghatékony megoldások, megoldási lehetőségek bemutatása. A biztonsági szint – ennek fényében – tovább növelhető, ha a fizikai kulcson kívül a belépésre jogosult személy biológiai egyedi tulajdonságai is validálásra kerülnek. Ez megvalósítható szoftveres modulok segítségével is.

A leggyakoribb billentyűzetes felhasználói felületen – mind nyomógombos, mind érintőképernyős kivitelben – alkalmazható az adatbeviteli eseményeket kísérő információ feldolgozása. A belépőre jellemző a billentyűk nyomva tartásának hossza és a gombnyomások vagy érintések között eltelt idő. Jellemző még a beviteli felület pontos helyének megnyomásától és a nyomás erősségétől függő rezgések egyénre jellemző vizsgálata is. A mérés elvégezhető egy gyorsulásérzékelő MEMS szenzor segítségével.

A jelszó beviteléhez köthető adatok felvételekor több minta vétele szükséges, ezekből meghatározhatók az egyes generált változókra elfogadható szélső értékek. Fontos figyelembe venni a felhasználó időbeli beviteli technikájának változását. Minden egyes belépéskor fontos lenne csúszóablakos elven tárolni a belépésre jellemző mért adatokat, és ezek alapján újra kalkulálni a megengedett szélsőértékeket. Az egyénre jellemző mért adatok szélsőértékből való kitérésekor, valamint a mért jellemző változásának dinamikájából fontos figyelmeztető, akár riasztást kiváltó esemény generálható.

Célszerű a három eltérő személyazonosítási elven alapuló módszer együttes, de egymástól független alkalmazása, a megbízható védelmi szint elérése érdekében.

3 Megvalósítás

Egy, a bemutatott megoldások tesztelésére szolgáló riasztórendszer modelljének rendszerterve a 8. ábrán látható. A központi mikrokontroller vezérli a köré épített modulokat, egységeket. [12]

Az érzékelők – jelen kiépítésben – egy zóna-duplázott vezeték szakadásérzékelésre és egy jelenlét érzékelésére alkalmas ultrahangos távolságmérő modult foglalnak magukba.

A felhasználói felület a kezelőn helyezkedik el, tartalmazza a felhasználó azonosítására alkalmazott RFID modult (jelen kiépítésben a rendszer élesítése és inaktiválása is ezen a felületen keresztül történik), egy LCD kijelzőt és a gyors állapot kijelzésére alkalmas státusz LED-eket. [13]

Az adatok küldése és fogadása a külvilág felé két csatornán lehetséges: vezetékes etherneten keresztül és/vagy GSM hálózaton keresztül.

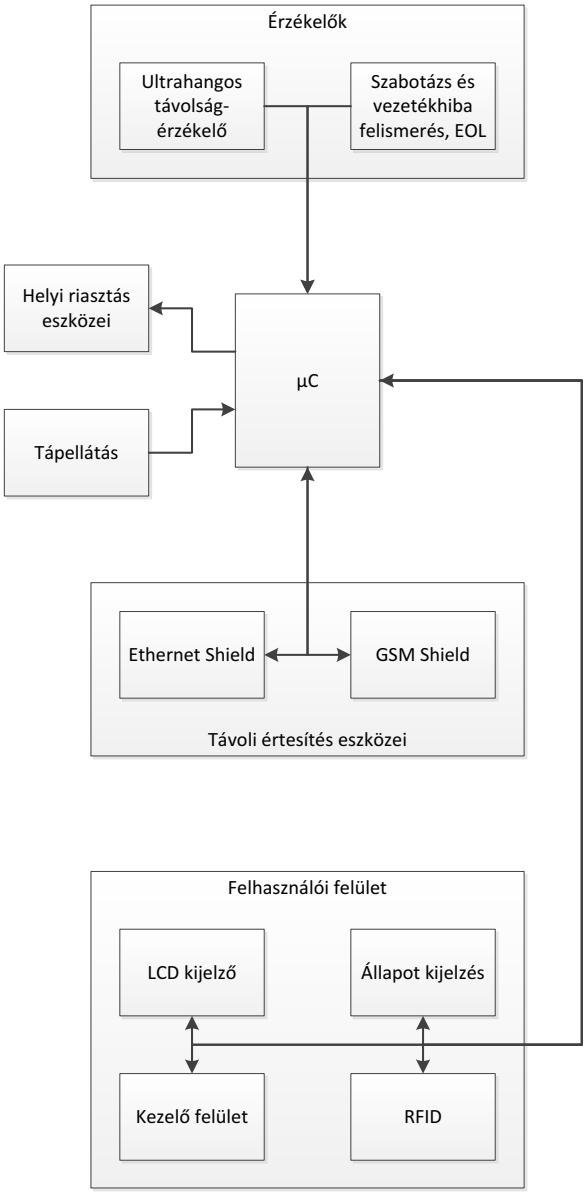
A riasztórendszer egyszerűsített, megépített modellje a 9. ábrán látható, az aktuális megvalósításban alkalmazott kiegészítő modulok az ábrán vannak jelölve.

A modellben alkalmazott ultrahang szenzor a HC-SR04. A szenzorba épített mikrokontroller a mért távolság függvényében változtatja a mintavételezés frekvenciáját a küldött és a fogadott jelek ütközésének elkerülése érdekében. (A kisebb távolsághoz nagyobb frekvencia társul.)

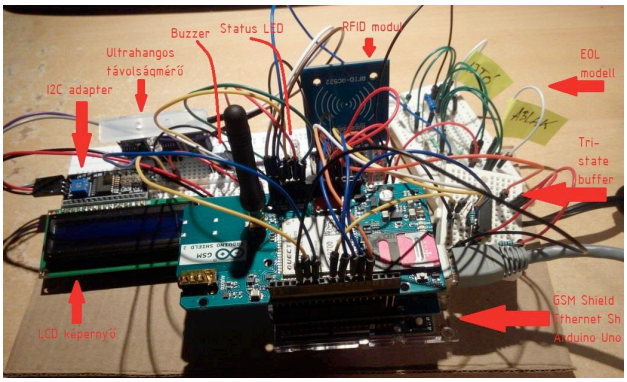
Az alkalmazott Ethernet shield és RFID író/olvasó modul is SPI buszon keresztül kommunikál a mikrokontrollerrel. Nehézséget jelentett az említett buszra kötött eszközök együttműködését hosszútávon, stabilan

biztosítani, ezért tri-state-es buffer fokozattal leválaszthatóvá tettem az eszközöket. Az Ethernet shield a buszról történő leválás után nem minden alkalommal tudott újra csatlakozni a rendszerhez.

A mikrokontroller bemeneti lábainak alacsony száma is korlátot jelentett a fejlesztés folyamán. Ez és az SPI busz megosztásának problémája vezetett el a továbbfejlesztett modell kialakításához, amiben két kontroller dolgozik külön feladatokon, de egymással kommunikálva. Az eddig is használt kontroller felel a külvilággal és a felhasználóval való kapcsolattartásért, az újonnan illesztett nagyobb lábszámú kontroller pedig az érzékelők lekérdezéséért valamint a riasztás és szabotázs érzékeléséért.



8. ábra: Rendszer architektúra



9. ábra: Megvalósított modell

4 Továbbfejlesztési lehetőségek

A hardver további bővítése mellett tervezem az említett szoftveres kiegészítő funkciók rendszerbe integrálását is. Miután a tervezett fejlesztések megtörténtek, szeretném vizsgálni a rendszer zavarállóságát is [14].

Véleményem szerint az egyedileg fejlesztett rendszerek megbízhatósága jelentősen nagyobb, mivel a behatoló nem képes a telepítés helyszínétől elkülönülve próbálkozni a rendszer megkerülésével, feltörésével – amennyiben a műszaki dokumentáció nem áll a behatolást tervező rendelkezésére.

Továbbá, szükséges még egy általános telepítői felület fejlesztése – amely csak telepítői jelszóval módosítható – a riasztórendszer könnyebb telepíthetőségének és testreszabhatóságának elősegítésére. A rendszer moduláris hardver és szoftver felépítése is támogatja az előirányzott fejlesztéseket.

5 Összefoglalás

A gyakran alkalmazott elektronikus vagyonvédelem által nyújtott hardverelemek és szoftveres megoldások mellet lehetőség van eddig még ritkán alkalmazott funkciók beépítésére is. Ezesetben cél a költségek alacsonyan tartása mellett egy komplexebb rendszer kialakítása, a biztonsági szint növelése. A bemutatott példák az előbbi feltételeket teljesítik az elektronikus kültéri védelem, a behatolást jelző rendszer és a beléptető rendszer esetében is. Az ajánlott megoldások relevanciája – a szerző reményei szerint – polgári és ipari területeken is jelentősek.

Irodalomjegyzék

[1] Berek Lajos. Biztonságtechnika. Budapest: Nemzeti Közszolgálati Egyetem. 2014. 48 p.

[2] György Györök, Bertalan Beszédes. Highly reliable data logging in embedded systems. In: Anikó Szakál, Iveta Zamecnikova. SAMI 2018: IEEE 16th World Symposium on Applied Machine Intelligence and Informatics : Dedicated to the Memory of Pioneer of Robotics Antal (Tony) K. Bejczy : proceedings. 237 p. Košice; Herlány, Szlovákia. 2018.02.07-2018.02.10. Seattle (WA): IEEE, 2018. pp. 49-54. ISBN:978-1-5386-4771-4

[3] Vass Attila, Berek Lajos. Napenergia és az elektronikai jelzőrendszer, villamos energia hálózattól távol lévő objektumok védelmének lehetőségei. HADMÉRNÖK 24:(2) pp. 41-57. (2015)

[4] Györök György, Bertalan Beszedes. Fault tolerant power supply systems. In: Orosz Gábor Tamás. 11th International Symposium on Applied Informatics and Related Areas (AIS 2016). Székesfehérvár, Magyarország. 2016.11.17. Budapest: Óbudai Egyetem. 2016. pp. 68-73.

[5] Doppler-effect. https://soundwavesreillymckennaaly.weebly.com/doppler-effect.html. (2018. május 13.)

[6] Continuous-wave radar. http://www.wikiwand.com/en/Continuous-wave_radar. (2018. május 13.)

[7] Fast Vibration Sensor Switch. https://andicelabs.com/shop/sensors/fast-vibration-sensor-switch. (2018. május 13.)

[8] http://www.nubbeo.com.ar/modulo-sensor-de-vibracion-sw420-tilt-arduino-nubbeo-549560390xJM (2018. május 13.)

[9] Piesoelectric sensor. https://en.wikipedia.org/wiki/Piezoelectric_sensor. (2018. május 13.)

[10] Michael A. Mahler, Qinghua Li, Ang Li. SecureHouse: A Home Security System Based on Smartphone Sensors. Department of Computer Science and Computer Engineering, University of Arkansas. IEEE International Conference on Pervasive Computing and Communications (PerCom). March 2017. https://www.researchgate.net/publication/313508127_Secure-House_A_Home_Security_System_Based_on_Smartphone_Sensors. (2018. május 13.)

[11] Muchen Wu, Parth H. Pathak, Prasant Mohapatra. Monitoring building door events using barometer sensor in smartphones. 2015 ACM International Joint Conference. September 2015. https://www.researchgate.net/publication/311490862_Monitoring_building_door_events_using_barometer_sensor_in_smartphones. (2018. május 14.)

[12] Dr. Györök György. Mikrokontrollerek hardver-hatékony alkalmazása. In: Nagy Rezső, Hajnal Éva. Garai Géza Szabadegyetem II. Székesfehérvár: Óbudai Egyetem, 2015. pp. 5-15. ISBN:978-615-5460-62-3

[13] Györök György. Programozható analóg áramkörök mikrovezérlő környezetben. Óbudai Egyetem, ISBN 978 615 5018 97 8, Budapest, 2013.

[14] Gy. Györök. A-class amplifier with FPAA as a predictive supply voltage control. In: 9th International Symposium of Hungarian Researcherson Computational Intelligence and Informatics (CINTI2008). 2008. 361–368. p.