Werner Gábor Á[302]: *A kritikus infrastruktúrák kockázatelemzési módszereinek újragondolása, különös tekintettel az ivóvízellátásra*

Absztrakt: Ebben a cikkben elsősorban a kritikus infrastrukúrák, avagy – a jelen megfogalmazás szerint – létfontosságú rendszerek kockázatelemzési metodikájának hátterét vizsgáltam meg. A nemzetközi és hazai jogszabályi háttér még nem kellően kiforrott, nincsenek olyan széleskörűen elfogadott szabványok, amelyek kellően pontos útmutatást nyújtanák a kockázatelemzők számára. A kritikus infrastruktúrák összetett hálózatának elemzése komplex feladat, nem vizsgálhatók külön, ennek következtében sok változót kell figyelembe venni, amik a többszörös kölcsönhatások következtében általában nem lineáris viszonyban állnak. A feladat összetettségéből kifolyólag indokolttá válik, hogy részletesebben megvizsgáljuk a lágy számítási módszerek alkalmazhatóságát, különösen a fuzzy logika adaptálhatóságát ezekben a rendszerekben.

Bevezetés

A kritikus infrastruktúrák meghatározása és szerepe

A Kritikus Infrastruktúrák (továbbikaban KI) védelme olyan közfeladat, amiben számos szereplő és érdekelt fél együttes fellépése szükségeltetik. Több nemzeti és nemzetközi definíció is létezik a KI meghatározására, érdemes az Európai Unió által használt megfogalmazást alapul venni. „*Az Európai Unió kritikus infrastruktúra védelemmel kapcsolatos folyamatában az infrastruktúra kölcsönösen egymástól függő hálózatok rendszere, amely magába foglalja az azonosított iparágakat, intézményeket (beleértve humán erőt és tevékenységet) és képességeket, amelyek gondoskodnak a termékek és szolgáltatások megbízható áramlásáról, a kormányok minden szinten történő zavaratlan működéséről és a társadalom egészéről*” [1].

Az utóbbi években a fogalom használata egyre szélesebb körben elterjedt, de a hétköznapi használatban sok esetben torzító hatásokat szenvedt el a tudományos értelmezés. A szóösszetétel mindkét tagjának jelentése a köznyelvben homályos értelmezéssel párosul. A hétköznapi értelmezéssel szemben az infrastruktúra alapvetően a gazdaságtanban alkalmazott kifejezés azokra a javakra, amik közvetve segítik a termelést, de direkt módon nem vesznek részt a javak előállításában, míg az infrastruktúra fogalma nem jelenti azt, hogy az adott eszköz, vagy létesítmény ingyenes vagy „állampolgári jogon jár”, sőt annak igénybevételét valamilyen módon a használó megfizeti, – *habár nem minden esetben egyértelmű, hogy ki milyen arányban használ egy-egy infrastrukturális elemet* –.

Az infrastruktúrák közé sorolhatjuk a műszaki infrastruktúra elemeit, tehát a telekommunikációs hálózatot, a közműhálózatot, az úthálózatot, a közlekedési csomópontokat, beleértve a kikötőket, reptereket, állomásokat és a közösségi közlekedést, valamint az ezeket kiszolgáló objektumok és eszközök hálózatát. Az infrastruktúra fogalmát tágabban értelmezve szokás idesorolni a közegészségügyet, a közoktatást valamint a szociális rendszert is, amelyeket „társadalmi infrastruktúrának” nevezünk. Bizonyos források – véleményem szerint megindokolhatóan – az infrastruktúrák közé sorolják a közbiztonság és katasztrófavédelem elemeit is.

Az infrastruktúra összetett definícióját tovább árnyalja a „kritikus” jelző értelmezése. A későbbiekben bemutatott definíciók egyéni értelmezése szerint kritikusnak nevezhető az az infrastruktúra, amelynek megszűnése vagy nem megfelelő (elégtelen) működése jelentős mértékben változtatja meg az általa ellátott terület működését. Sajnos a „jelentős” jelző fogalmát nem könnyű meghatározni. Jellemzően olyan hatást tekinthetünk jelentősnek, amely akut módon veszélyezteti a

[302] Óbudai Egyetem, Alkalmazott Biometria Intézet wga.bme@gmail.com

társadalom életminőségét és a gazdasági stabilitást, vagy az államrend megbomlását idézheti elő. Mind a szakirodalom, mind a hétköznapi szóhasználatban előfordul a „létfontosságú" jelző is, mint a „kritikus" szinonimája.

Európai dokumentumok a kritikus infrastruktúrák védelmében

Az Európai Unió a Zöld Könyv szerint a következők módon definiálja a kritikus infrastruktúra fogalmát: „*azok a fizikai eszközök, szolgáltatások, információs technológiai létesítmények, hálózatok és vagyontárgyak tekinthetők kritikus infrastruktúrának, amelyek megrongálása vagy elpusztítása súlyos hatással lenne az európaiak egészségére, békéjére, biztonságára, vagy gazdasági jólétére illetve az EU és a tagállamok kormányainak hatékony működésére*"[303]. Emellett két szintjét határozza meg a kritikus infrastruktúráknak; úgymint az intranacionális és a határokon átnyúló hatással bíró, úgynevezett „európai kritikus infrastruktúrák". A hatás tekintetében az a mérvadó, hogy okozhat-e jelentős kárt az infrastruktúra sérülése más tagállamnak.

Ezzel szemben a magyar jogszabályok szerinti értelmezés már valamivel konkrétabb: „*kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában.*" [2]

Mindezek alapján, Magyarországon „*kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére.*" [304]

A kritikus infrastruktúrák meghatározása tehát függ attól, hogy az adott intézmény mekkora területet lát el, illetve a nem megfelelő működésből fakadó hatások milyen gyorsan és milyen mértékben multiplikálódnak a környezet, társadalom és gazdaság hármasában. A kifejezés viszonylag új keletű, bevezetését az indokolta, hogy valamilyen módon meg kell kellett határozni azoknak az infrastrukturális intézményeknek (szolgáltatásoknak) a körét, amelyek sérülése nemzet (esetleg nemzet feletti) biztonsági szinten jelentős kockázatot jelentenek. Ennek következtében tulajdonképpen már a kritikus infrastruktúrák kijelölését is meg kell, hogy előzze egy kockázati felmérés, amely iteratív jelleget kölcsönöz a teljes folyamatnak.

1. ábra: A Kritikus Infrastruktrák kockázatelemzésnek körfolyamata

[303] Az Európai Unió Zöld Könyve alapján (Green Paper on European Programme for Critical Infrastructure Protection COM(2005) 576 final).

[304] 2080/2008. (VI. 30.) kormányhatározat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról (1. sz. melléklet – Zöld Könyv a kritikus infrastruktúrák védelmére vonatkozó nemzeti programról).

A kétezres évek elején, az Amerikán és Európán végigsöprő terrorhullám következtében a jogalkotók is felismerték, hogy valamilyen módon meg kell határozni a kritikus infrastruktúrákra vonatkozó követelmények rendszerét, és elejét kell venni annak, hogy a szándékos támadások vagy a véletlen balesetek jelentős nemzetbiztonsági kockázatot jelentsenek. E törekvések szellemében született dokumentumokat az alábbiakban foglaltam össze.
A madridi (2004. március 11.) és londoni (2005. július 07.) terrortámadások után Európa is rádöbbent, hogy a polgárok biztonságérzete és biztonsága is ki van téve a kritikus infrastruktúrák sebezhetőségének. A hadviselés jellege alapjában változott meg, mert a „frontvonal" akár metróperonon is húzódhat. A megszületett dokumentumok három kérdés megválaszolása mentén formálódtak. Egyfelől fel kellett mérni, hogy mik a kritikus infrastruktúrák és mik a potenciális veszélyek, másfelől arra is választ kellett adni, hogy milyen preventív és milyen reaktív lépéseket lehet tenni a kockázatok csökkentése érdekében, harmad részről pedig meg kellett vizsgálni, hogy Európa szerte hogyan tudják az egyes érintett kritikus infrastruktúrák értesíteni egymást, és együttműködni a kockázatmenedzsmentben?
Az Európai Bizottság 2004 októberében közleményt[305] adott ki a terrorizmus elleni harc és a kritikus infrastruktúrák védelmének összefüggéseiről, majd röviddel ez után, még 2004 decemberében az Európai Tanács elfogadta „**Létfontosságú Infrastruktúrák Európai Programjának**" (European Programme for Critical Infrastructure Protection – EPCIP) elkészítésére vonatkozó előterjesztést. Ebben kijelölték a terrorizmus elleni harc főbb irányvonalait, úgymint a nemzetek közti együttműködés erősítése, az európai határok megerősített védelme, a terroristákat finanszírozó és támogató elemek felderítése, a polgári védelem fejlesztése [1].
Az Európai Parlament 2005 júniusában a „**lambririndis javaslat**" [306] alapján kiadta ajánlását a kritikus infrastruktúrák védelmével kapcsolatban. Néhány nappal a londoni támadássorozat után a tagállamok képviselői kihangsúlyozták elkötelezettségüket a terrorizmus elleni harcban és a kritikus infrastruktúrák védelmében. A fenti törekvések eredményeként az Európai Bizottság 2005 novemberében jelentette meg a kritikus infrastruktúrák védelmére vonatkozó európai programról szóló „**Zöld Könyvet**" [307] [1].

A **Zöld Könyv** keretdokumentumként fogalmazza meg az EPCIP alapvető fogalmait, irányelveit és módszertanát. Kitér a módszeres és teljes körű kockázatelemzésre és kockázat menedzsmentre, a felülvizsgálatokra és egészében vizsgálja a kritikus infrastruktúrák hálózatát, figyelembevéve az interdependenciális[308] kapcsolatokat. A Zöld Könyv mint uniós direktíva pozitív fogadtatásban részesült a tagállamok részéről, de se tagállami se közösségi szinten nem fogalmazott meg konkrét intézkedéseket, és nehézségeket jelentett a határokon átnyúló hatások elemzése, ezért 2008 decemberében az Európai Unió Tanácsa elfogadta az európai kritikus infrastruktúrák azonosításáról és biztonsági felméréséről szóló **114/2008. EK Irányelvet**, aminek kapcsán megjelent egy nem kötelezően alkalmazandó kézikönyv, az Irányelv alkalmazásáról. Az Irány elv egyik legfontosabb újítása, hogy rendszeres felülvizsgálatot és jelentési kötelezettséget ír elő a tagállamok számára.
Fontos megjegyezni, hogy olyan program esetében, mint az EPCIP különösen fontos, hogy a mind a tagállamok, mind a kritikus infrastruktúrák üzemeltetői könnyen és biztonságosan értesíthessék egymást és szükség esetén kommunikálhassanak egymással. Ezen igények kielégítésére hozták létre 2009 januárjában a **Kritikus Infrastruktúrák Figyelmeztető Információs Hálózatát** (Critical Infrastructure Warning Information Network – CIWIN[309]). A rendszer két lényeges tulajdonsága, hogy

[305] COM(2004)702 – közlemény a kritikus infrastruktúrák védelméről a terrorizmus elleni küzdelemben
[306] 2005 januárjában Stavros Lambrinidis, görög európai parlamenti képviselő kezdeményezésére, a Hágai Programot és a közös biztonsági stratégiát üdvözölve egy konkrétabb, egyértelműbb célkitűzéseket tartalmazó javaslat került kidolgozásra, amely egy többéves kutatási projekt megkezdését szorgalmazza a tagállamokban és az unió területén található létfontosságú infrastruktúrák sebezhetőségének
[307] COM(2005)676 – Zöld Könyv az EPCIP-ről
[308] Kölcsönös függés, két állandó egység közötti állandó viszony
[309] A Tanács határozata a létfontosságú infrastruktúrák figyelmeztető információs hálózatáról (CIWIN)– COM(2008) 676 final

lehetőség van az élőidejű riasztás továbbítására, valamint minősített tartalom megosztására, a legjobb gyakorlatok és a felmerülő problémák kapcsán [1].

Hazai szabályozások és rendelkezések a kritikus infrastruktúrák védelmében

Ahogy minden uniós szinten vezérelt ágazatban, az uniós direktívákat át kellett ültetni a magyar jogszabályokba, mégpedig úgy, hogy azokkal mindenkor összhangban legyenek. A EPCIP irányelve szerint minden tagállamnak fel kellett mérnie saját kritikus infrastruktúráit, sebezhetőségeit és a potenciális veszélyforrásokat. Fontos szempontként jelent meg, hogy a lakosságot be kell vonni a katasztrófakezelésbe, amivel elérhető a kockázat passzív csökkentése. A lakosság veszélyhelyzetekre[310] esetleg szükségállapotra[311] történő felkészítése segíti a kritikus infrastruktúrák elégtelen működéséből, sérüléséből fakadó kockázatok minimalizálását [1].

A Katasztrófavédelmi Tudományos Tanács (KTT) kiadványában foglaltak alapján a „*jelenlegi hazai és nemzetközi biztonságpolitikai álláspontok szerint, Magyarország terrorfenyegetettsége alacsony, belső társadalmi rendje kiegyensúlyozott, természeti katasztrófák általi veszélyeztetettsége főként hidrológiai eredetű. Mindez elég okot szolgáltat arra, hogy hazánk integrálja jogi és tevékenységi folyamataiba a kritikus infrastruktúra védelem uniós programjának célkitűzései.*" [1].

Nem tartom szükségszerűnek a hazai szabályozás részletes ismertetését az uniós jogharmonizáció előtti időszakról, ennek tükrében az ismertetést a **Magyar Zöld Könyvvel** kezdem. Az uniós csatlakozást követően a magyar ágazati egyeztetéseken is kiderült, hogy meg van az igény az európai Zöld Könyv implementálására. A KTT munkáját ismét idézve megfogalmazásra került, hogy „*a hazai zöld könyvben megfogalmazott célkitűzések szerint a kritikus infrastruktúra védelem a kockázatok azonosításán alapuló megelőzés, az érintettek bevonásával megvalósuló felkészülés és az ellenálló képesség fejlesztésének hármas rendszerében működő mechanizmus, amely nem irányul minden veszélyeztető tényező elleni védelemre, hanem tudatos elemzések és meglévő tapasztalatok alapján célirányosan garantálja a megfelelő védelmi szintet. Az EPCIP-ben felsorolásra került alapelveket a hazai adaptálás során a nemzetközi szerződésekből fakadó kötelezettségek elvként történő meghatározásával egészítették ki annak érdekében, hogy Magyarország eleget tudjon tenni NATO szövetségesi feladatainak is*" [1].

A fentiek tükrében megszületett a magyar Nemzeti Kritikus Infrastruktúra Védelmi Program (továbbiakban NKIV) és ennek jogszabályi háttere a **2080/2008. (VI. 30.) kormányhatározat**. A kormányhatározat strukturált és viszonylag jól áttekinthető formában megjelöli, hogy mik tekinthetőek ma Magyarországon kritikus infrastruktúrának, melyik minisztérium a felelős az érintett területen. A kormányhatározatban az alapelvek definiálása mellett megjelenik a potenciális veszélyek (szándékos, természeti és civilizációs) kategorizálása is.

Annak ellenére, hogy viszonylag pontosan meghatározott jogi hátteret sikerült a hazai EPCIP mögé állítani, a gyakorlatban nem kezdődtek el az ágazatközi párbeszédek. Ahogy az uniós direktívának való megfelelési kötelezettség határideje közeledett, a párbeszédek felelőségi körei tisztázása céljából megszületett **a 1249/2010. (XI. 19.)** ***kormányhatározat*** *az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végrehajtandó kormányzati feladatokról*. A kormányhatározat a belügyminiszter, a nemzeti fejlesztési miniszter és a honvédelmi miniszter számára fogalmazza meg pontosan a felelősségi köreiket, emellett meghatározta egy munkacsoport felállítását is, amely az uniónak küldendő jelentés rendszeres összeállításával foglalkozik. A kormányhatározat alapján jött létre 2011 áprilisában a **Kritikus Infrastruktúra Védelem Konzultációs Fórum** (KIV KF), melynek célja egy új módszertan megalkotása és a döntések előkészítése, támogatása. A fórumot kiegészítve, de vele szorosan együttműködve alakult meg 2011 szeptemberében a KIV KF **Polgári Védelmi Munkacsoport**, melyek kifejezetten a polgári védelem szempontjából vizsgálja a szükséges lépéseket [1].

---

[310] A **veszélyhelyzet** a szükséghelyzetet el nem érő mértékű, az élet- és vagyonbiztonságot vagy a környezetet veszélyeztető természeti csapás, illetőleg ipari baleset okozta állapot (Pvtv.mehatározása szerint).

[311] A **szükségállapot** olyan helyzet, amelyben emberek egy nagyobb csoportjának egészsége, élete, tulajdona vagy a környezet közvetlen veszélynek van kitéve.

A kritikus infrastruktúrákat meghatározó **2080/2008. (VI. 30.) kormányhatározat** ágazati felsorolásának negyedik pontjában jelennek meg az ivóvíz-szolgáltatáshoz kapcsolódó ágazati szereplők, melyek a következők; ivóvíz szolgáltatás, felszíni és felszín alatti vizek minőségének ellenőrzése, szennyvízelvezetés és –tisztítás, vízbázisok védelme és árvízi védművek, gátak.
Az NKIV programja az ivóvíz-szolgáltatás területén a **2080/2008. (VI. 30.) kormányhatározat** szerinti struktúrában épült fel, miszerint a védelem három pilléren nyugszik, amelyek a megelőzés, a felkészülés és az ellenálló képesség. A kormányhatározat szövegével élve ezek a következőképpen értelmezendők:
„***Megelőzés és védelem**: kritikus infrastruktúrák jelentős kihatású meghibásodásának vagy teljes leállásának hatékony megelőzése a kritikus infrastruktúrák és azok legnagyobb kockázatot képviselő elemeinek beazonosításán, kijelölésén, a kockázatok elfogadott legkisebb mértékűre történő csökkentését biztosító elemzések lefolytatásán és a szükséges védelmi intézkedések alkalmazásán keresztül.*"
„***Felkészülés és jelzés**: az infrastruktúra tulajdonosok, üzemeltetők és az állami szervek megfelelő felkészítésének biztosítása a kritikus infrastruktúra meghibásodása vagy működésének megszakadása esetére.*"
„***Üzemfolytonosság és ellenálló képesség**: jelentős kihatású meghibásodás vagy kiesés, teljes leállás esetén a működés lehető legrövidebb időn belül történő visszaállítására, illetve helyettesítő megoldások alkalmazására irányuló képességek, intézkedések tervezése, kialakítása, végrehajtása és fejlesztése."*
A jogszabályban is megfogalmazottak szerint a védekezés nem az ivóvíz-szolgáltatás „*kis kihatású működési zavaraira*", vagy az „*infrastruktúrákra veszélyt jelentő összes tényezőt kizáró teljes védelemre*" irányul, hanem a „*sebezhető pontok csökkentésével, valamint a kockázati tényezők tudatos felmérésével és beazonosításával biztosítja a kritikus infrastruktúrák számára a megfelelő védelmet*". Ezzel szemben, az ivóvíz-szolgáltatás területén igenis teljes körű védelemre kell törekedni mind a hazai, mind a nemzetközi szakmai gyakorlat szerint.

A fenti irányelv által kijelölt út mentén az országgyűlés 2012 novemberében elfogadta a **2012. évi CLXVI. törvényt**, *a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.* A törvény célja egyfelől kritikus infrastruktúrák – avagy a törvény által újonnan bevezetett terminológia szerint a „*létfontosságú rendszerek*" – elemeinek azonosítása, megfelelő kijelölése és a védelem és biztonság megvalósítása. Ennek keretében a Lrtv. az alapfogalmak definiálásán túl, rendelkezik az európai és nemzeti kritikus infrastruktúrák kijelöléséről, az **üzemeltetői biztonsági terv** elkészítésének kötelezettségeiről, a **biztonsági összekötő személyéről**, valamint az **ellenőrzés szabályairól és a szankciókról**. A Lrtv. végrehajtásának érdekében született a 65/2013. (III. 8.) kormányrendelet, amely részletesen megadja azüzemeltetői biztonsági terv tartalmi és formai követelményeit, valamint a létfontosságú létesítmények horizontális kritériumait.
A létfontosságú rendszerek és létesítmények azonosítása során körvonalazódott azon rendszerek és rendszer-elemek köre, amelyeket a jövőben a BM OKF hivatott ellenőrizni és koordinálni. E kötelezettség részeként a hálózatbiztonsági elvárások teljeítése érdekében lépett hatályba az *elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjának, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről szóló 233/2013. (VI. 30.) kormányrendelet*.
„*Fenti feladatok ellátására a BM OKF megtette az első lépéseket. 2013. március 19-én átadásra került és megkezdte működését az Országos Iparbiztonsági Főfelügyelőség keretein belül a **Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja** (LRLIBEK), egyelőre elsősorban iparbiztonsági események kezelésével, gyakorlatok, ellenőrzési akciók koordinálásával. Emellett folyamatosan bővíti a hálózatbiztonsági szakmai tevékenységet és a bevont rendszerek körét, és kialakítja a működési protokollokat, szabályrendszereket. Az LRLIBEK a magyar és nemzetközi hálózatbiztonsági szervezetektől a **Kormányzati Eseménykezelő Központon** keresztül kapott riasztások kezelésére – a nemzeti létfontosságú rendszerek és létesítmények érintettsége*

esetén – számítástechnikai sürgősségi reagáló egységként működik folyamatos rendelkezésre állással.” [312]

A jogszabály külön definiálja a létfontosságú információs rendszereket és létesítményeket: *„a társadalom olyan hálózatszerű, fizikai vagy virtuális rendszerei, eszközei és módszerei, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek, vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek.”* [313]

Az LRLIBEK feladatai közé sorolhatóak a fenti rendszereket és hírközlő hálózatokat a cybertérből érő támadások elhárításának koordinálása, a rendszeres tájékoztatás és információnyújtás a nemzeti létfontosságú rendszerelemként azonosított informatikai rendszerek és hírközlő hálózatok felé a felismert és publikált sérülékenységekről, más szervezetektől átvett információk és adatok alapján az érintett létfontosságú rendszerek üzemeltetőinek értesítése, és a megelőzés érdekében a szükséges technikai lépések elvégzése, illetve az ágazati szereplők képzése.

Az eseménykezelő központ tulajdonképpen nagymértékben hozzájárul, hogy a CIWIN-ben megfogalmazott nemzetközi elvárások megvalósulhassanak. A kritikus infrastruktúrákra jellemző, hogy összetett informatikai hálózattal rendelkeznek, ami felelős a rendszerirányítás, a monitoring és a biztonsági feladatokért is. Ezen hálózatok sokszor a TCP/IP rendszer hálózati rétegein keresztül továbbítják az információt. A hálózatok topológiája természetesen alapjaiban meghatározhatja a védelem struktúráját, azonban a jelen filozófiája szerint a szeparált rendszereket is közvetlen módon kell csatlakoztatni az eseménykezelő központhoz. Ennek következtében lehetőség nyílik olyan külső támadásra, ahol nem elsősorban a klasszikus biztonságtechnikai eszközök, hanem az cybernetikai védelem jut szerephez [2].

A védelmi intézkedések és a biztonságtechnikai rendszerek kialakítása során tehát még összetettebb kockázatelemzési és -értékelési rendszert kell kialakítani. Ki kell térni a hagyományos támadásokra a rongálástól a mérgezésig, de hasonlóan fontos az adatok és információk védelme és az informatikai rendszerek integritásának megőrzése. Ahogy a vizsgálandó szempontok száma növekszik, úgy válik összetettebbé és átláthatatlanabbá a rendszerek működése. Nagy rendszerek esetében, jellemzően ilyenek a több-százezres városokat vagy annál nagyobb településeket, településrészeket ellátó kritikus infrastruktúrák, az elemzésbe bevont elemek száma és a források és hatásviselők közti viszony összetettsége erősen indokolja, hogy újragondoljuk a kockázatelemzés módszertanát.

További problémaként említhető, hogy a törvény által meghatározott **üzemeltetői biztonsági terv**, amely korábban a vízművek életében, mint **vízbitonsági terv** szerepelt pontosan meghatározza a kötelező elemeket és azok bemutatásának módját, azonban nem nyilatkozik arról, hogy milyen módszerekkel és technikai megoldásokkal kell megvalósítani a KI védelmének megtervezését és megvalósítását. E tekintetben hiányosság tapasztalható a biztonsági és védelmi intézkedéseket meghatározó vállalati irányelvek, szakmai szabványok és a létfontosságú rendszerekre vonatkoztatott jogszabály viszonyában is. A jogszabály definiálja a kockázatelemzés fogalmát, miszerint; *„fenyegetettségi és kockázati tényezők vizsgálata a rendszerelemek sebezhetőségének, valamint a megzavarásuk vagy megsemmisítésük által okozott következmények értékelése céljából”* [314], de nem ad kielégítően pontos útmutatást vagy ajánlást a kockázatelemzés lefolytatásához.

A hatályos jogszabály nem hivatkozik szabványokra, ennek oka elsősorban arra vezethető vissza, hogy **nincs olyan nemzeti vagy uniós szabvány, ami az érintett infrastruktúrák működését közvetlenül szabályozná**. A tapasztalat azt mutatja, hogy a részterületeken alkalmazható szabványok és a vállalati önkéntes szabályozások segítik az üzemeltetési biztonsági terv elkészítését, sőt bizonyos pontokba lefedik a törvény által előírt kritériumokat, de mégsem érvényesül egy általános biztonsági

[312] Belügyminisztérium, Országos Katasztrófavédelmi Főigazgatóság

[313] 65/2013. (III. 8.) kormányrendelet, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

[314] 65/2013. (III. 8.) kormányrendelet, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

szemléletmód, és nincs olyan szakmai útmutatás, ami megfelelően pontos és számonkérhető vizsgálati módszereket valamint technikai megvalóításokat követelne meg.

Az ivóvíz-szolgáltatásban régóta létezik önálló jogi szabályozás, a legtöbb kritikus infrastruktúra esetében azonban el kell ismerni, hogy az uniós direktíva és annak átültetése hozta meg a kívánt jogszabályi változásokat. Az ivóvíz-szolgáltatás területén már rendelkezésre álló ajánlások és előírások – a jó gyakorlatokat illetően – nemzetközi szinten először az Egészségügyi Világszervezet kiadványaiban jelentek meg. Ezek átültetése az „üzemeltető biztonsági tervbe" viszonylag jól elvégezhető, analógiája azzal egészen hasonló.

A vízművek mint KI kockázatelemzési módszerei

A módszerek háttere, alapelvek

Az Egészségügyi Világszervezet 2004-es Kézikönyve felhívta rá a figyelmet, hogy az ivóvíz minőségének megőrzése érdekében kockázat alapú Vízbiztonsági tervet kell készíteni. Sorra kell venni minden kockázatot a teljes rendszerre, a vízgyűjtőtől a kifolyókig [3].

A TECHNEAU által a kockázat kezelési- és vízbiztonsági tervekhez 2007-ben kiadott keretdokumentum és módszertan meghatározza a kockázat alapú értékelés elméletét, és az alább taglalt módszertanokat is összehasonlítja. A módszertanok csoportosítása során megkülönbözeti a kvalitatív módszereket, amik elsősorban ellenőrzőlistákon és biztonsági szintekbe soroláson alapulnak, biztosítva a listák relatív rangsorolását, és a kritikus kockázatcsökkentési pontok meghatározását, valamint a kvantitatív módszereket, amelyek lineáris számításokon alapulnak. A kifinomult, számszerű összehasonlítás megkönnyíti a becsült kockázati szintek és a megállapított tolerancia szintek összehasonlítását. A kvantitatív döntéselemzési módszerek megkönnyítik a kockázatcsökkentési intézkedések stratégiai elemzését, például a beruházások kompromisszumos rangsorolását a kockázatcsökkentés érdekében [4].

2. ábra: Integrált kockázat menedzsment sémája a VBT-ben (forrás: TECHNEAU)

A keretdokumentum nem fogalmaz meg olyan általános kockázatkezelési módszert, amely az összes vízmű esetében alkalmazható lenne a stratégiai és operatív döntések során, ellenben a következő támpontokat nyújtja [5]:

- Elvek a jó kockázatkezelési gyakorlathoz
- Releváns eszközkészlet a szükséges kockázatértékelés és kezelés elvégzéséhez
  - TECHNAU Veszély Adatbázis
  - Kockázatelemzési módszerek
  - Döntéstámogató eszközök
  - Világos gyakorlati példák a kockázatelemzés alkalmazásából

A **kockázatkezelés** fogalma kiterjed az egész vízbiztonsági tervezésre, a rendszerfelmérésétől a beavatkozásokig mindent magában foglal. A **kockázatvizsgálat** viszont már szűkebb értelemben foglalkozik a kockázatokkal, tulajdonképpen a **kockázatelemzését** és **kockázatértékelését** jelenti. A kockázat-vizsgálat és a kockázat-csökkentés, valamint az ellenőrzés együtt jelenti a kockázat-kezelést. De mit is jelent valójában a kockázat? Stan Kaplan szerint három tényező határozza meg [6]. A kockázat egyfelől függ attól, hogy *„mi történik?”*, másfelől, hogy *„mekkora valószínűséggel?”*, és harmadszor, hogy *„mik a következményei?”*. A modern kockázatelemzések során a Kaplan-i definíciót – nem feltétlenül helyesen – úgy értelmezik, hogy milyen események, mekkora valószínűséggel és milyen súlyos hatásokat előidézve fordulhatnak elő.
A kockázatvizsgálat során az első lépés a kockázatelemzés. A **kockázatelemzés** felméri és dokumentálja a veszélyeket, illetve további elemzési, intézkedési döntéseket határoz meg. A kockázatelemzést követően értékelni kell a felmerülő kockázatokat. Az **kockázatértékelés** fő feladata eldönteni, hogy a felmerülő veszélyek a továbbiakban elfogadhatóak-e, vagy sem. A veszélyek értékelését azonban a különböző érdekeltek nem azonos módon látják. A többdimenziós érdekek megkívánják, hogy olyan elvek és kritériumok alapján értékeljük a veszélyeket, melyeket az érintettek, hatásviselők bevonásával határoztak meg. Itt felmerül többek közt két probléma; az immissziós hatások nehéz detektálhatósága, és az externális hatások forrásainak ismeretlensége. Több elv is létezik, amelyek alapján a kockázatokat értékelhetjük, az egyik legalapvetőbb az **ALARP** (As Low As Reasonably Practicable), ami azt hangsúlyozza, hogy olyan alacsony szintű kockázatot fogadjunk el, ami ésszerűen lehetséges [4].
Ennek alapján néhány könnyen elfogadható kockázattal a továbbiakban nem kell foglalkoznunk. Az elfogadható és nem elfogadható kockázatok között azonban lesz egy nem is olyan keskeny sáv, ahol a technikailag vagy gazdaságilag ésszerűen nem csökkenthető kockázatok állnak. A kitétellel elfogadott kockázatok elvét az **ALARA** (As Low As Reasonably Achievable) fogalmazza meg, amely szerint csak olyan alacsony kockázat fogadható el, ami ésszerűen elérhető [4].
A többdimenziós érdekek olyan matematikai módszereket követelnek meg, amelyek kellően könnyen tudnak alkalmazkodni, az érdekek közti különbségekhez és azok esetleges változásához. A matematika hagyományos, kockázat-vizsgálatokban alkalmazott módszerei azonban ezt nem képesek minden esetben kielégíteni. Vizsgálataim egyik fő témája, hogy miként lehetne a mesterséges intelligenciát e területen alkalmazni.

Az alkalmazott módszerek bemutatása

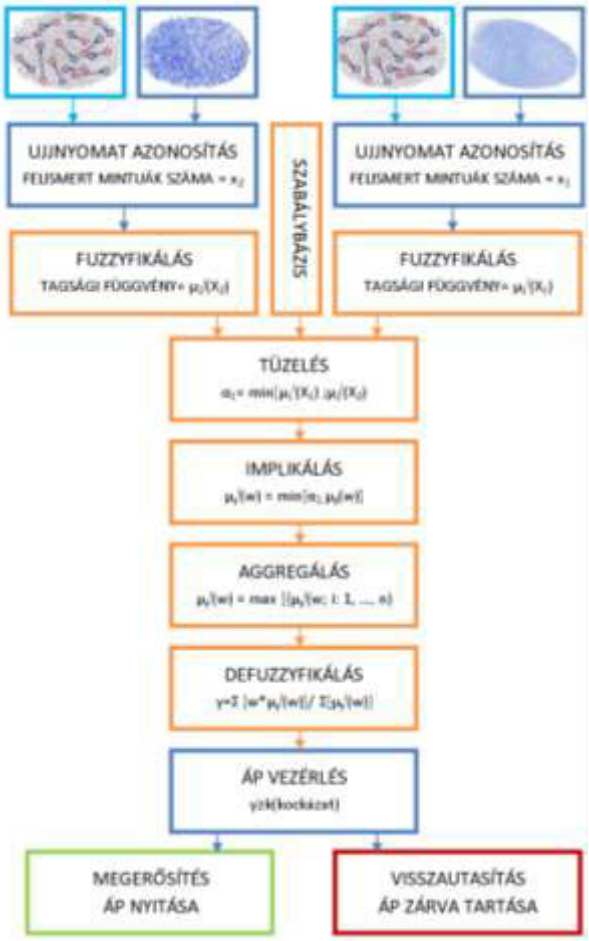
A kockázatelemzés során alkalmazott módszerek mind a tervezés mind a működés fázisában alkalmazhatóak és alkalmazandóak. A lágy számítások összetettebb matematikai háttere azonban nehezen lenne kellően szemléltethető egy általános elméleti módszertan bemutatása során. Ebből kiindulva a klasszikus kockázatelemzési módszerek többnyire teoretikus bemutatásával szemben szeretném a fuzzy logika egy gyakorlati alkalmazhatóságát felvázolni.
A biztonságtechnikai alkalmazások során különösen fontos lehet e logika alkalmazása. Régóta jelent problémát az, hogy a beléptető rendszerek milyen biometrikus jellemzőket vizsgáljanak, és azokat „milyen mértékű vizsgálatnak” vessék alá. Bizonyos esetekben nem találunk hatékonyabb megoldást – szem előtt tartva a költségeket, az üzembiztonságot és a megtéveszthetőséget –, mint egy „portás” alkalmazását. Mi lehet az oka annak, hogy egy ismerten sok hibával működő humán eszköz a korlátok teljes skáláját figyelembe véve megbízhatóbb működésre képes, mint egy biometrikus azonosító rendszer?
A fenti kérdésemre az egyik lehetséges válasz az, hogy a „portásunk” képes a fuzzy logika alkalmazására, míg egyelőre a biometrikus azonosítás a gyakorlatban nem jutott el ide. A „portás” folyamatosan multimodális elemzést végez, amit a fuzzy logikához hasonló gondolkodással értékel, és ez alapján már kellő biztonsággal és hatékonysággal képes ellátni munkáját. Természetesen nem állítom, hogy egy biometrikus rendszernél biztonságosabb vagy megbízhatóbb lenne egy „portás” alkalmazása, csak azt feltételezem, hogy a rendszerek jelenlegi korlátaiknál fogva nem képesek olyan összetett döntések meghozatalára, mint az élő erős védelem. A biometrikus azonosító rendszerek jelenlegi egyik legnagyobb hátránya az, hogy általában egyetlen jellemzőt képesek mérni, amelyet

esetleg hordozott azonosítóval vagy PIN kóddal erősíthetőek. A biometrikus azonosításban sokáig az az elv volt az uralkodó, hogy elegendő egy egyedi azonosítót „tökéletes” – a célnak megfelelő – pontossággal mérni. Ma már inkább több jellemzőt, vagy egy jellemző több felületen történő mérését tekintik az új iránynak. A több jellemzős („multimodális”) mérések elve már némiképpen közelít az emberi logika interpretálásához, de fontos, hogy milyen matematikai eszközzel vetjük össze a különböző faktorok eredményeit. A legtöbb esetben a vezérlő számítógép programja több faktort vizsgál meg és kiszámítja a megfelelőségek középértékét, majd amennyiben a közép megfelel egy előzetesen beállított értéknek, akkor engedélyezi a belépést, ezzel szemben a fuzzy logikánál nem diszkrét értékek elemzése és utólagos átlagolása történik, hanem a faktorok elemzése összevonódik [7] [8].
Amennyiben a fuzzy logika alapján vetjük össze a jellemzőket, lehetőségünk nyílik a hozzárendelési szabályok általi finomhangolásra, vagy akár a dinamikus változtatásra, amely növeli a rendszerek rugalmasságát. Sőt a szakirodalom elképzelhetőnek tartja az olyan rendszereket is, amelyek adaptálódnak a környezet változásaihoz neurális hálózatok és genetikus algoritmusok segítségével. A könnyebb szemléltetés végett, elsősorban ujjnyomatok vizsgálatával foglalkoztam, de a szakirodalomban több olyan tanulmánnyal is találkozhatunk, amelyik a meglévő módszerek különböző kombinációjával, vagy a gyakorlatban még nem alkalmazott biometrikus azonosító eszközökkel foglalkozik, esetleg kombinálja a fuzzy logika alkalmazását a kriptográfiával és az adatkezeléssel [9][10][11].
Konkrét vizsgálataim arra irányultak, hogy összehasonlítsam az ujjnyomatok azonosítása során felismert minutiák számának alakulását, annak érdekében, hogy a fuzzy logika alkalmazásával a multimodális megoldások csökkenthetik-e a sikeres azonosításhoz szükséges minutiák számát. Hiszen ezzel a technikával a beléptetés gyorsítható, a hordozó felület változása – a bőr öregedése, koszolódása, stb. – bizonyos szinten tolerálható, mindamellett, hogy a kockázati szint nem változik.

Eredmények, gyakorlati alkalmazhatóság

Kétségtelen, hogy a legszélesebb körben alkalmazott biometrikus azonosítási módszer az ujjnyomatok ellenőrzése, hiszen a bűnügyi azonosításban már több mint százéves története van. A digitális technika fejlődésével a felismerés folyamatát a beléptetési rendszerekben automatizálták, így védett objektumokban, bizonyos államok határain, de akár hétköznapokban is találkozhatunk már ujjnyomat-olvasókkal. E dolgozatnak nem célja a biometrikus azonosítást végző eszközök bemutatása, vagy azok működésének részletes ismertetése, mert a későbbiekben prezentált vezérlési folyamat azoktól elválasztva történik meg. Ennek szemléltetésére tekintsünk az alábbi blokkábrára.

A 3. ábrán egy bimodális, ujjnyomat érzékelőkkel párosított kialakítást tüntettem fel, a faktorok száma azonban bizonyos szintig növelhető és igény szerint módosítható a vizsgálandó biometrikus jellemző. A bizonyítás során azért választottam az ujjnyomatokat, mert a minutiáik értékelésének viszonylag széles körben elfogadott módszertana van. Az összehasonlításnál pedig nyilvánvalóbb a két azonos jellemző mérésén alapuló módszertan különböző kiértékelési módszere közti különbség igazolása.



12. ábra: Fuzzy logika alapú irányítási rendszer blokkséma

Belátható tehát, hogy a bemeneti eszközök változtathatóak, de figyelembe kell venni, hogy a felismert egyedi azonosító jegyek számának milyen az eloszlása. A fuzzy logika „zavart" karakterisztikájából adódóan több ponton is lehetőség van a vezérlési folyamat programozására. Befolyásolhatjuk a szabályrendszert, a tagsági függvények karakterisztikáját és számát, az aggregációs szabályokat, és a defuzzyfikálás függvényét, valamint annak értelmezését. A kísérleteim a nemzetközi szakirodalommal összhangban azt mutatták, hogy vannak olyan programozási pontok, amelyek hatása nem különösebben változtatja meg a végeredményt, míg vannak olyan paraméterek, amelyek igen nagy hatással vannak az eljárásra. Ezen tulajdonságok következtében további vizsgálatok természetesen abszolút indokolttá váltak, hiszen fontos megismerni, hogy miképpen lehet optimalizálni a vezérlés működését.

A kritikus infrastruktúrák, mint a civil és a kormányzati objektumok közti átmenet különleges biztonságtechnikai rendszereket igényelnek, hiszen a veszélyeztetettség magas, de a biztonsági rezsimintézkedések nem hátráltathatják az operatív működést [12].

A kockázat-adaptív rendszerek fejlesztése azért vált indokolttá, mert sok intézmény – *akár kormányok is* – és multinacionális nagyvállalat (nemzet) biztonsági és titokkezelési okokból kifolyólag nem képes megfelelően gyorsan feldolgozni, megosztani és elterjeszteni az érzékeny információkat, annak ellenére, hogy ezek segítenék a külső eseményekre történő gyors és hatékony válaszlépéseket. A legnagyobb nehézséget e rugalmatlan rendszerek számára a környezeti ingerek és szükségletek dinamikus kezelése jelenti. Egyes események megértésének és a hatékony válaszlépések megfogalmazásának feltétele lehet a különböző osztályok (szervezeti egységek) információinak összevonása [10].

A tapasztalatok alapján a probléma az, hogy a beléptető rendszerek – *ahogy minden biztonságtechnikai eszköz* – kompromisszumokat jelentenek. Olyan eszköz nem létezik, ami egy adott

célra tökéletes, de meg lehet találni azt az eszközt, ami a biztonsági irányelveinknek a legmegfelelőbb. Véleményem szerint a probléma nem az, hogy az adott eszköz mekkora kompromisszumot jelent, hanem a nehézségeket az jelenti, hogy a biztonsági politikában rögzített elvárásoknak a megváltozott körülmények és igények mellett mennyire képes alkalmazkodni [12].
A Fuzzy logikát alkalmazó többszintű biztonsági szisztémának (Fuzzy Multi Level Security – Fuzzy MLS) legfőbb célja az, hogy olyan biztonsági rendszert hozzon létre, ami ösztönzi az információk megosztását és a megfontolt kockázatvállalást a felhasználók számára, hogy a szervezet/intézmény maximalizálni tudja a rendszerei (vállalatirányítási, könyvelési, környezetvédelmi, stb.) előnyeit, miközben minden felhasználó továbbra is felelős a tetteiért, és a lehetséges sérülések – melyek az információ kiszivárogtatásából fakadnak – minimalizálva vannak. Emellett a szervezet képes lesz a kockázatos információ áramlása során az operatív szükségletek, kockázatviselés és a környezet változásait dinamikusan adaptálni [12].

Ahogy azt már korábban írtam, egy szervezet – *a mi esetünkben egy kritikus infrastruktúra* – külső és belső fenyegetésekkel szemben is fel kell, hogy készüljön. A technikai oldalról általában a belső fenyegetések jelentik a nagyobb veszélyt, mert a támadó ismeri a rendszer bizonyos elemeit, esetleg működését, vagy akár a hozzáféréssel is rendelkezik bizonyos eszközökhöz, zónákhoz. Általában nincs rá lehetőség, hogy egy civil szervezet nyomonkövesse az alkalmazottak elő- és utóéletét, ezért minden alkalmazottra úgy kell tekinteni, mint egy potenciális támadóra. E koncepciót erősíti az a feltevés is, hogy a kritikus infrastruktúrák esetében az alkalmazottak tudatos zsarolását és a kihasználását is, mint potenciális veszélyforrást kell figyelembe venni. Fontos, hogy az alkalmazottak jogosultságainak mind személyi, mind térbeli, mind időbeli korlátai legyenek. Tehát a kérdés nem az, hogy KI, MIKOR és HOL van, hanem, hogy KI, MIKOR és HOL lehet. A Quantified Risk–Adaptive Access Control – továbbiakban QRAAC –, azaz a numerikus kockázat-adaptív beléptető rendszerek segítenek választ találni arra a kérdésre, hogy a sikeres és hatékony működéshez, milyen mértékben kell átalakítani a biztonsági rendszerek irányelveit, sőt kvantitatív módon adnak becslés a kockázati értékek megváltozásáról.
A Fuzzy MLS rendszerek hasznosítják és kiterjesztik a logikus kockázat alapú MLS rendszerek modelljét, de a hozzáférési jogosultságokat a kockázat menedzsment modellje szerint változtatják meg. Ebben a tekintetben megjelenik a dinamikus és adaptív jogosultság kezelés. Példának okáért tegyük fel, hogy egy kritikus infrastruktúra szigorúan titkos minősítésű objektumában olyan vészhelyzet alakul ki, amit a helyi erők nem tudnak kezelni (tűzeset, biológiai, vagy kémiai támadás, stb.). Tudjuk, hogy a beléptető rendszereknek biztosítani kell a megfelelő menekülési utakat is, de ezzel együtt továbbra is szem előtt kell tartani az integritás védelmének kérdéseit. Tehát a vészhelyzet kezelésére érkező személyeknek és csak is nekik, azonnal belépési jogosultságot kell adni. A jogosultság ellenőrzéséhez szükséges időt azonban minimalizálni kell, aminek egyik lehetséges megoldása a fuzzy logikára épülő multimodáláis biometrikus azonosítás. E rendszerek egyik kritikus feltétele, hogy CIWIN hálózatában a biometrikus sablonok titkosított formában, de bármikor, bármelyik áteresztési ponton elérhetőek legyenek [12][13].
Ahogy a nemzetközi szakirodalmak is rávilágítottak, a gyakorlatban egyre nagyobb igény jelentkezik olyan vezérlési és irányítási módszerek iránt, amelyek a nem lineáris és összetett matematikai kapcsolatokat is képesek kezelni.

Referenciák

[1] Katasztrófavédelmi Tudományos Tanács Pályázata: A Kritikus Infrastruktúra Védelem Fogalmi Rendszere, Hazai és Nemzetközi Szabályozása, Budapest, 2011
[2] Cristina Alcaraz, Angel Balastegui, and Javier Lopez: EarlyWarning System for Cascading Effect Control in Energy Control Systems, Computer Science Department - University of Malaga, 29071 - Malaga, Spain
[3] World Healt Organisation (2004): Guidelines for Drinking-water Quality, Vol. 1:3rd ed., ISBN 92-4-154638-7

[4] L. Rosen, P. Hokstad, A. Lindhe, S. Sklet, J. Røstum (2007): Generic Framework and Methods for Integrated Risk Management in Water Safety Plans; Chalmers Inivertsits of Technology, SINTEF, TECHNEAU

[5] Dr. Papp Mária, Dávidné dr. Deri Matild, Bódi Gábor, Dr. Solti Dezső, Solymosi Ernő, Havas András (2007): MAVÍZ kézikönyv, Távlati Vízigények Elemzése

[6] Kaplan, S. (1997): The Words of Risk Analysis, Risk Analysis Volume 17, Issue 4, pages 407–417., DOI: 10.1111/j.1539-6924.1997.tb00881.x

[7] Stephen Price-Francis (1998): Biometric identification process and system utilizing multiple parameters scans for reduction of false negatives, US5815252 A

[8] I. Iancu, N. Constantinescu, M. Colhon (2010): Fingerprints identification using a fuzzy logic system, Int. J. of Computers, Communications & Control, ISSN 1841-9836, E-ISSN 1841-9844 Vol. V (2010), No. 4, pp. 525-531

[9] V.S.Meenakshia, Dr.G.Padmavathib (2010): Security Analysis of Password Hardened Multimodal Biometric Fuzzy Vault with Combined Feature Points Extracted from Fingerprint, Iris and Retina for High Security Applications, Procedia Computer Science 2 (2010) 195–206

[10] Mohamad Abdolahi, Majid Mohamadi, Mehdi Jafari (2010): Fingerprints Identification using a Fuzzy Logic System, Int. J. of Computers, Communications & Control, ISSN 1841-9836, E-ISSN 1841-9844 Vol. V (2010), No. 4, pp. 525-531

[11] T. Takedaa, K. Kuramotoa,b, S. Kobashia,b, Y. Hataa,b (2011): Fuzzy-logic is precise - Its application to biometric system, Scientia Iranica D 18 (3), 655–662

[12] Pau–Chen Cheng, Pankaj Rohatgi, Claudia Keser, Paul A. Karger, Grant M. Wagner, Angela Schuett Reninger (2007) Fuzzy Multi–Level Security :An Experiment on Quantified Risk–Adaptive Access Control, Security and Privacy, 2007. IEEE Symposium p. 222 – 230., ISSN 1081-6011 ISBN 0-7695-2848-1

[13] Mohamad Abdolahi, Majid Mohamadi, Mehdi Jafari (2013) Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic; International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013