MMXIV. II. ÉVFOLYAM IV. SZÁM

NEMZETBIZTONSÁGI SZEMLE

KÜLÖNLENYOMAT

NEMZETI KÖZSZOLGÁLATI EGYETEM
NEMZETBIZTONSÁGI INTÉZET
BUDAPEST

Műholdas rendszerek EMP elleni védelme

Szűcs Péter[1]

Absztrakt:

Az előző cikkemben a tanult elektronikai hadviselési módszerek és a kutatásaim során feldolgozott szakirodalom alapján vizsgálva bemutattam a műholdas távközlési rendszerek támadási módjait az alternatív vagy humán fegyverekkel és eljárásokkal, valamint az elektronikai zavaró megoldásokkal. Ezen írásomra támaszkodva megvizsgálom, hogy az EMP[2] ellen hogyan védhetők a műholdas kommunikációs rendszerek.

Kulcsszavak: *műholdas kommunikáció, ASAT rendszer, Faraday elv*

Abstract:

In my previous article, measured by the electronic warfare methods learned and processed in the research literature presented ways to attack the satellite communications or human weapons and alternative procedures, and the annoying electronic solutions. Based on this paper I examine how it can be protected against EMP satellite communications systems.

Keywords: *satellite communication, ASAT system, Faraday principle*

[1] *szucs.peter@nbsz.gov.hu*

[2] *Electromagnetic pulse - Nagyenergiájú elektromágneses impulzus*

Bevezetés

Kutatási témám az információs társadalom által használt kommunikáció egy szeletét vizsgálja, vizsgálom a műholdas személyi távközlési rendszerek felderíthetőségét, és a dolgozatomban tárgyalom ezen rendszerek védelmi lehetőségeit a fizikai támadásokkal, elektronikai hadviselési tevékenységekkel szemben. Jelen cikkemben arra vállalkozom, hogy az általam felkutatott szakirodalom, valamint az elektronikai hadviselés ismereteim tükrében választ, vagy válaszokat adjak a kérdésre.

Az USA felső katonai vezetése 2013-ban vizsgálta a katonai műholdas kommunikációs rendszerek fenyegetettségét, és a következő megállapításra jutott: Meg kell védeni a műholdas távközlési rendszerüket a különféle támadásokkal szemben, továbbra is fenntartani az információs fölényt. Az amerikai védelmi szféra - értékelve műholdas rendszereit - a fenyegetési formákat három csoportba sorolta[3]:

1. Fizikai támadások (ütközések, vagy létfontosságú alkatrészek tönkretétele, amely lehet irányított is egy arra alkalmas támadó műhold segítségével (pl: Kína ASAT program[4]), vagy irányított energiát alkalmazó támadások, mint például a nagy teljesítményű lézerek és mikrohullámú rendszerek, amelyek tönkreteszik a kritikus műholdas elemeket, mint például a napelem és érzékelők. Egy másik típusú fizikai támadás, amelyik nem közvetlenül a műholdra irányul, hanem a földi infrastruktúra támadásával-tönkretételével éri el a kommunikáció ellehetetlenítését, azonban az előző módszernél jóval olcsóbban.
2. Elektronikai támadások, amelyek egyaránt támadhatják a rendszerek műholdas, felhasználói – és földi szegmensét az uplink és downlink csatornák zavarásával.
3. Kiber-támadás a műholdak irányításának átvétele, a műhold átmozgatása egy másik pályára, vagy akár a műhold által használt

[3] Options for Military Satellite Communications Debated http://www.spacepolicyonline.com/news/options-for-military-satellite-communications-debated (letöltve: 2014. 01. 11.)

[4] ASAT,,parazita műhold" néven emlegetett programon a kínai űrkutatási akadémia (CAST) kis műholdak kutatóintézete dolgozik.

üzemanyag-ellátás megakadályozása, vagy károkozás a fedélzeti elektronikában.

Az általam vizsgált műholdas rendszerek mindegyike működési szempontból három alapvető részre tagolható, bontható. A támadhatóság és védelmi megoldások taglalásához továbbra is ezt a modellt kívánom használni. Ezek a részek a következők:

1. Műholdas szegmens, amely magába foglalja a LEO (Low Earth Orbit), MEO (Medium Earth Orbit), vagy a GEO (Geosynchronous Earth Orbit) pályán keringő távközlési műholdakat.
2. Földi szegmens, amely magába foglalja a műholdak irányítását, távvezérlését és pályán tartásának elemeit, illetve azokat a földi átjátszó állomásokat, amelyek összekapcsolják a műholdas rendszert a földi infrastruktúrával.
3. Felhasználói szegmens, amely magába foglalja a műholdas kommunikációs eszközökön kommunikáló felhasználói készülékeket.

A műholdas rendszerek EMP elleni védelmét az elektronikai hadviselés tevékenység részeként tárgyalom, melynek alapvető célja az ellenség katonai információs rendszereinek elektronikai úton való támadása, illetve a saját hasonló rendszerek működésének biztosítása, az élőerő és a csapatok megóvása. Eszerint az elektronikai hadviselés támadó (offenzív) és védelmi (defenzív) oldalait tudjuk megkülönböztetni.[5]

Az elektronikai hadviselés a következő három, egymást kiegészítő, valamint egymást részben átfedő területre osztható:

- elektronikai támogatás (Electronic Support Measures – ESM);
- elektronikai ellentevékenység (Electronic Counter Measures – ECM);
- elektronikai védelem (Electronic Protection – EP).[6]

Az EMP elleni védelem az elektronikai védelem egyik passzív módja, melynek definíciója a következő: „*az elektronikai védelem az elektronikai hadviselés azon területe, amely biztosítja az elektromágneses spektrum saját részről történő hatékony használatát az ellenség elektronikai támogató és ellentevékenysége, va-*

[5] *Prof. Dr. Haig Zs.-Prof. Dr. Kovács L.-Dr. Ványa L. Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata, Felderítő Szemle Budapest X. évfolyam 1-2. szám, 2011. március-június, HU ISSN 1588-242X (pp.: 183-207)*

[6] *uo.*

lamint a saját csapatok által okozott nem szándékos (kölcsönös) rádiózavarok előfordulása ellenére."[7]

Az elektronikai védelem csökkenti, vagy lehetetlenné teszi az ellenségnek a frekvenciaspektrum feletti fölény megszerzésére irányuló törekvéseit. Az elektronikai védelmi tevékenységek védelmi természetűek és természetszerűleg jóval többet jelentenek, mint az elektronikai rendszerekbe tervezett és beépített technikai lehetőségek összességét. Az elektronikai védelem a felderítés és az elektronikai ellentevékenység – ezen belül a saját nem szándékos interferenciák – megakadályozására irányuló aktív és passzív tevékenységek, módszerek és rendszabályok alkalmazását, bevezetését jelenti.[8]

Ahhoz, hogy a műholdas kommunikációs rendszereinket megvédjük a fent említett fenyegetésekkel szemben alapvetően négy kérdésre kell választ adni:

1. Milyen rendszert kell megvédeni?
2. A fenyegetés függvényében a rendszer melyik eleme a legsérülékenyebb?
3. Milyen szintű védelem szükséges a normál működés biztosításához?
4. Az elégséges, vagy szükséges szintű védelemhez rendelkezünk-e az anyagi forrásokkal?

A válasz mind a négy kérdésre szubjektív, de úgy gondolom, hogy a lenti passzív- és aktív védelmi megoldásokkal kielégítő választ adhat a kérdésekre. A fenti definíció alapján két módszer lehetséges az elektronikai támadásokkal szemben, a passzív- és aktív védelmi módszerek alkalmazása. A passzív védelem lehetővé teszi, hogy a rendszer túlélje a támadásokat, biztosítja a normál működést, az aktív védelem feladata pedig, hogy megzavarja a támadást.

Passzív védelmi megoldások[9]

Frekvencia ugratásos szórt spektrum (FHSS)[10] használata. A műholdas kommunikációs rendszerekben az adatjelet egy keskenysávú vivőre ültetik rá, s ennek a vivőnek a frekvenciája igen rövid időszakonként - másodpercenként többször - széles sávban megváltozik, "ugrik". A változások véletlenszerűnek tűnnek, de a kapcsolatban álló felek számára a szekvencia előre ismert. Az FHSS techni-

[7] *uo.*

[8] *uo.*

[9] *Todd Harrison: The Future Of Milsatcom 2013 Center for Strategic and Budgetary Assessments.*

[10] *Frequency-hopping spread spectrum*

kának a jellegéből következően igen jó az interferenciatűrő képessége. A műholdas rendszerek felmenő és lejövő jeleinek zavarvédelmét javítja.

Fedélzeti jelfeldolgozás. A rendszer zavarvédelmét növeli, csökkenti a műholdakon az elektronikai zavarást azáltal, hogy a demodulálást és dekódolást a műholdon végezzük el, és csak ezután sugározzuk vissza a jelet. A rendszer képes a felmenő jelek hibáinak felismerésére és javítására.

Hibajavító kódolás alkalmazása. A hibafelismerés az adó és a vevő közötti átvitel folyamán a zaj vagy egyéb zavar okozta rendellenességek miatti torzulások jelzésére és kijavítására szolgáló algoritmus.

Műholdak közötti közvetlen jeltovábbítás. A földi állomások a támadás szempontjából a legsérülékenyebbek, ezért ha a műholdak közötti jeltovábbítást alkalmazzuk, tovább javíthatjuk a rendszerünk zavarvédettségét. Természetesen a műholdak közötti kommunikáció megteremetése igen bonyolult és költséges műszaki megoldásokat kíván (lásd IRIDIUM rendszer működése). A feladó földi állomás jele mindaddig a műholdak között továbbítódik, míg el nem éri hívott állomást, jel csak ekkor érkezik vissza a fogadó földi állomásra.

EMP védelem. Jelen írásom következő fejezetében a műholdas passzív védelmi eljárások közül az EMP elleni védelmi móddal kívánok foglalkozni. Az általam vizsgált szakirodalom alapján az EMP hatása kiemelkedő károkat okozhat a műholdas rendszer elemeiben – főleg a földi- és felhasználói szegmensben - a többi támadási móddal ellentétben.

Adat titkosítás. A rendszerben továbbított információk védelmére tikosítanunk kell az átviendő információkat. A MILSATCOM rendszerekben erre fejlesztették ki az úgynevezett AEHF képességet, amely az adattovábbítás legfejlettebb titkosításával lehallgatás, illetve a zavarással szembeni ellenállóságot biztosítja.

Aktív védelmi megoldások[11]

Shoot –Back. A műhold fel lesz szerelve egy nagyteljesítményű lézer fegyverrel, amellyel képes magát megvédeni az ASAT műholdakkal szemben. Ez a védelmi rendszer azonban ellentmondhat a kis súly és egy képesség egy műholdon elvnek, amelyet a következő fejezetben mutatok be. A fejlesztőknek foglakozniuk kell a fenti negyedik kérdés megválaszolásával is, amely a bekerülési költségekről szól.

Védő, kísérő műholdak. Nem minden műhold rendelkezne védelmi képességgel, hanem az alkalmazott műholdpályákon, sávokban elhelyezett kísérő műhol-

[11] *Todd Harrison: The Future Of Milsatcom 2013 Center for Strategic and Budgetary Assessments.*

dakkal védik a többi műholdat. Csak ezek a műholdak rendelkeznének támadó képességgel.

Manőverező képesség. Olyan műholdak kifejlesztése, amelyek a magukkal vitt üzemanyag révén korlátozott manőverezési képességgel rendelkeznek.

A szakirodalomból tudott, hogy ez szabja meg a műhold élettartamát és egyben kihat az költségekre is.

Műholdas rendszerek EMP hatás elleni védelme

A jövő műholdas kommunikációjának fejlődési trendjei azt mutatják, hogy egyre nagyobb a valószínűsége, hogy a katonai és civil műholdas rendszerek integrálódnak, ezért szükségük van különböző szintű katonai védelemre. Meg kell védeni Őket a különböző fizikai-, elektronikai-, és kiber támadásokkal szemben. Ebben a fejezetben az általam feldolgozott szakirodalom alapján vizsgálom és bemutatom a földi állomások EMP elleni védelmi technikáit. Az EMP pusztító hatás fizikája az elektromágneses indukció elvén alapul. A nagysebességű térerősség ugrás minden vezetőben villamos feszültség indukál, ami a szigetelések átütéséhez, a félvezető rétegek belső szerkezetének átégéséhez vezet. Az elektronikai eszközök fejlődése, a félvezetők egyre nagyobb számú elterjedése a túlfeszültséggel szembeni sérülékenység növekedésével járt. Amíg egy elektroncsövet csak több száz, vagy ezer V feszültséggel lehetett tönkretenni, addig ma egy 3 V alatti feszültséggel működő processzornak a 10V is végzetesen nagy feszültség.

Az elektromágneses impulzusok elleni védelem alapvető problémája, hogy a védett eszköznél nem ismert az elektromágneses impulzus nagysága. Így nehéz megállapítani, hogy milyen nagyságú elektromágneses impulzust kell lecsökkenteni olyan mértékre, amelyet még károsodás nélkül elviselnek az érzékeny elektronikai eszközök. A szükséges érték ismeretében lehetőség lenne meghatározni azt az optimálisan szükséges védelmi módszert és eszközt, így nem kellene minden esetben a maximális védelmi értéket biztosító eljárást vagy eszközt alkalmazni.

Két alapvető módszer létezik az elektromágneses impulzusok elleni védelemre. Az egyik, hogy olyan elektronikai áramköröket építenek az eszközökbe, amelyek ellenállnak az elektromágneses impulzus hatásainak, a másik pedig, hogy árnyékolással megakadályozzák, hogy az elektromágneses impulzus bejusson a védett térbe. Természetesen az a legjobb, ha mindkét módszert egyszerre alkalmazzuk, mivel ez adja a legnagyobb védelmet.

Az elektromágneses impulzusok elleni védelem eszközeinek széles választéka létezik.

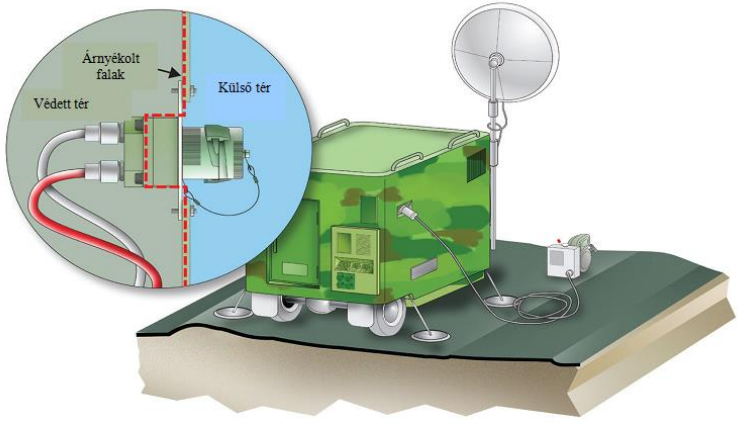
Ezek a teljesség igénye nélkül az alábbiak lehetnek:

- szikraközös villámhárító eszközök; Két elektróda között szigetelőrétegként levegő helyezkedik el. Alaphelyzetben az elektródák között a szigetelőréteg miatt nem folyhat áram, ezért ez az állapot a kapcsoló nyitott helyzetének felel meg. Ha az elektródák közötti feszültséget emeljük, akkor elérjük azt a feszültséget, amelyen bekövetkezik az átütés, és elektromos ív alakul ki. Az ív nagyon kis ellenállású elektromos összekötésnek tekinthető, ezért ez az állapot a kapcsoló zárt helyzetének felel meg. Az átütési feszültséget az elektródák távolsága határozza meg: úgy állítják be, hogy az átütés hamarabb következzen be a szikraközben, mint a védett fogyasztóban.
- hálózati szűrők; Kiszűrhetők az adathálózaton terjedő zajok, zavarok és túlfeszültségek, amelyek a tápegységek, adatátviteli eszközök korai meghibásodásához vezethetnek.
- elektrooptikai eszközök; Az elektrooptikai átalakítás révén nagy zavarvédettségre tehetünk szert, hiszen az elektromos jel optikai jellé történő átalakításával - a rádiófrekvenciás spektrum egy magasabb tartományába lépésével - a nagy frekvenciájú impulzusok hatásmechanizmusa nem érvényesül. A gondot továbbra is az elektromos jel optikai jellé, illetve ennek inverzét átalakító eszközök jelentik, védelmükre koncentrálva csökkenthető a probléma.
- nagy sebességű zener diódák; Működése azon alapszik, hogy belső ellenállását igen gyorsan megváltoztatja (rövidre zár) ha a rákötött feszültség hirtelen megnövekszik, illetve átlépi a meghatározott küszöbszintet.
- árnyékoló és elnyelő anyagok; Ideális védelem biztosítható az elektromágneses impulzusok ellen. Az elektromágneses hullámok elleni árnyékolás módszerei lehetnek abszorbeáló (elnyelő) - és reflektáló (visszaverő) árnyékolás.[12]

[12] *Haig Zsolt-Kovács László: Kritikus infrastruktúrák és kritikus információs infrastruktúrák Tanulmány 2012 Nemzeti Közszolgálati Egyetem pp. 243-245 http://kovacsx.hu/download/doktorikepzes/KOVASZ_KII_Tanulmany_FINAL.pdf (letöltve: 2014. 05. 04)*

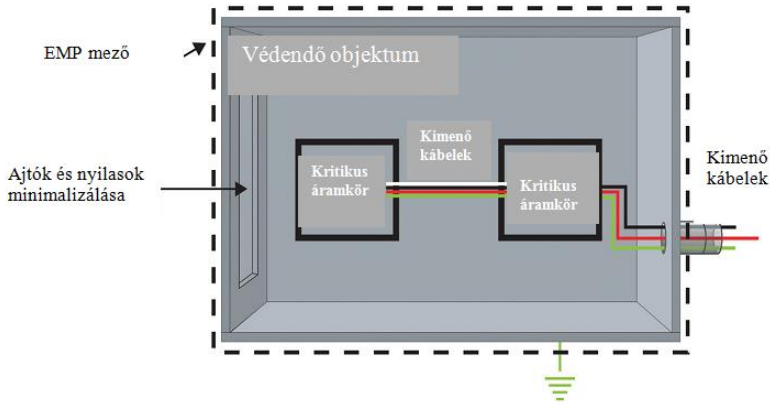
Az elektronikai hadviselési eszközök közül a legnagyobb fizikai pusztító erővel az úgynevezett EMP hatást alkalmazó fegyverek bírnak. Cikkemben továbbra sem tárgyalom a klasszikus kinetikus energiájú fegyvereket.

Az EMP hatás, vagy a hasonló elektromágneses kisugárzások ellen tehát a már fent említett árnyékolás, vagyis az úgynevezett Faraday elv nyújt védelmet, amelyre a védelmi szféra már szabvánnyal rendelkezik. A lényeg, hogy a fémtestben kialakított üreg belsejébe a külső elektromos mező nem hatol be. A külső fémburok megosztott töltései ugyanis a külső eredetű elektromos mezőt a fémtesten belül nullára változtatja. Minthogy a megosztás jelensége rendkívül gyorsan zajlik le, megállapíthatjuk, hogy a külső mező gyakorlatilag egyáltalán nem hatol az üreg belsejébe. Ezt a hatást nevezzük árnyékolásnak. Ha egy berendezést meg akarunk védeni az elektromágneses mezőktől, fémházba helyezzük, árnyékoljuk (1. ábra). Az lenti ábrán is látható, hogy árnyékoló hatás védi a fémből készült katonai műholdas földi állomásban dolgozó katonákat a viharban a villámoktól, de az EMP hatása ellen is. Sűrű szövésű fémharisnya védi az adók, vevők, erősítők, rádiók vezetékeit az elektromos zavaroktól. Hasonlóan védik a lőporraktárakat is a villámcsapástól. A fémburkolatot rendszerint földelik, hogy állandóan földpotenciálon legyen. Tehát a Faraday-kalitka az elektromágneses hatás kiküszöbölésére szolgáló, fémhálóval körülvett térrész, amelybe a fémháló védőhatása folytán a külső elektromos erőtér nem hatol be („árnyékolás”).



1. ábra Földi állomás Faraday kalitka katonai kialakítása[13]

[13] *System Approach to EMP Mitigation http://www.protectiongroup.com/ProtectionTechnologyGroup/media/PTG/WhitePapersandTechnicalNotes/1474-000.pdf (letöltve:2014.04.15)*



2. ábra Földi állomás Faraday kalitka kialakítása[14]

A Faraday-kalitka hatékonysága függ a kalitkát alkotó vezetőszálak közötti távolságtól (minél kisebb a távolság, annál biztonságosabb), függ a vezetők ellenállásától (minél kisebb, annál biztonságosabb), valamint a levegő pára-, por- és iontartalma is befolyásolja a hatékonyságát.[15]

Olyan civil és katonai kialakítás kell, amely megfelelő védelmet nyújt az óriási fezsültség és áram tranziensekkel szemben. A tranziensek között is különbséget kell tenni. A védelmi rendszernek különbséget kell tenni a bekapcsolási tranziens és a támadó tranziens között, biztosítva a megfelelő működést. Meg kell tervezni minden alkotó elemet a tömítéseket, a kimenő- és bemenő vezetékeket, a nyílászárókat, a tápellátáson keresztül a szellőzésig (lásd 2-3. ábra). A hatékonyabb védelem érdekében a nyílászárók számát lehetőség szerint minimalizálni.

A védelem szempontjából négy elem szinte kötelező:

- árnyékolás,
- földelés,
- szűrés,
- túlfeszültség-védelem.

[14] *System Approach to EMP Mitigation http://www.protectiongroup.com/ProtectionTechnologyGroup/media/PTG/WhitePapersandTechnicalNotes/1474-000.pdf (letöltve:2014.04.15)*

[15] *uo.*

A belső tér és a külső tér közötti védelemért a szűrő áramkörök felelősek. Feladatuk, hogy a kimeneti-bemeneti pontokon a védett térbe, illetve az elektronikus alkatrészekhez ne jussanak akkora feszültségek, amelyek az alkatrészek, és ezen keresztül a földi állomás tönkremeneteléhez vezetne.[16]

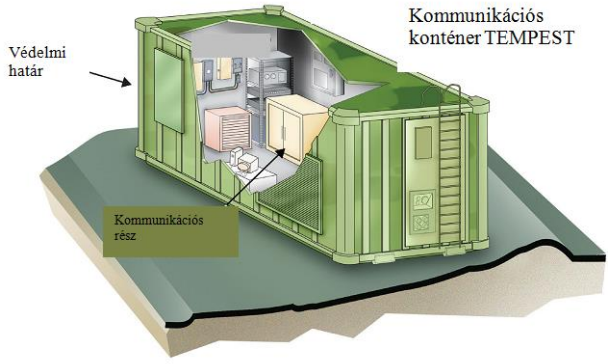
Az elektronikai elemek közül elsősorban a félvezetők érzékenyek a túlfeszültségre. A legegyszerűbb meghibásodási okok:

- Feszültség átütés: a meghibásodási mechanizmus a lavina átütés, az ehhez tartozó feszültség a szennyezés koncentrációtól függ.
- A helyi túlmelegedés következtében létrejövő megolvadás. A bipoláris eszközök meghibásodása kb. 90 %-ban szigetelő rétegek átütése és csak 10 % a vezetősávok megolvadása miatt következik be. A MOS technológiájú eszközökben viszont 60 %-nál nagyobb arányban fordul elő a fémezések olvadása és kisebb mértékű a dielektrikumok átütésének gyakorisága.

A villamos kisülések következtében az alkatrészek közül a nagy bemenő impedanciájú elemek már kisebb energiák esetén is tönkremennek. A félvezető alkatrészek közül nemcsak a FET, MOS és a CMOS eszközök, hanem a bipoláris elemek is sérülékenyek. Katasztrofálisan meghibásodhatónak a nagy bemenő ellenállású műveleti erősítők, az A/D konverterek is. A nagy bemeneti impedancián (pl. pF-nál kisebb nagyságrendű bemeneti kapacitás és igen nagy ohmos komponens esetén) a fellépő nagy feszültség átüti a vékony oxid rétegeket. De a bipoláris elemek p-n átmenetének kis impedanciája sem jelent előnyt, mert ezen viszont már kisebb feszültség esetén is nagy áram folyik át, ha egy feltöltődött test kapacitása azon keresztül sül ki. A nagy áram hatására ilyenkor termikusan üt át egy átmenet, vagy akár megolvadhat egy fémezés.[17]

[16] *uo.*

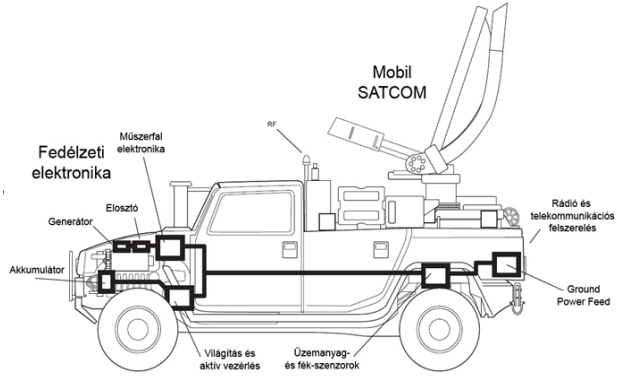
[17] *Farkas György: Készülékek zavarvédelme 2008 Győr pp.:1-51 http://www.sze.hu/~farkasgy/EMC-konyv/EMC1.doc (letöltve:2014.04.15)*



3. ábra Kommunikációs blokk konténeres kiépítése[18]

A felhasználói szegmens védelmi technikái

Ebben a fejezetben bemutatom, hogy az EMP hatás ellen hogyan védhetők a felhasználók kommunikációs eszközei és járművei. A kritikus elektronikára, főleg a C4I (vezetés, irányítás, kommunikáció, számítógép és az felderítés) rendszerek védelmére kell fordítani a legjobb képességeket. A C4I elemeket a gépjárművön belül egy szűk kamrában, más néven Faraday pajzsban kell elhelyezni, és a gépjárművet is el kell látni kiegészítő védelmi elemekkel.



4. ábra: C4I gépjármű HEMP védelme.[19]

[18] *System Approach to EMP Mitigation http://www.protectiongroup.com/ProtectionTechnologyGroup/media/PTG/WhitePapersandTechnicalNotes/1474-000.pdf (letöltve:2014.04.15)*

[19] *EMP Mitigation. Protecting Land Mobile Vehicles from HEMP Threat Environment*

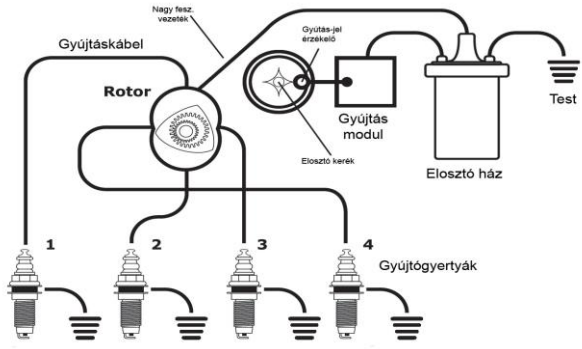
Ahhoz, hogy megtudjuk, hogyan tartsunk mozgásban egy járművet EMP (elektromágneses impulzus) támadás alatt, meg kell vizsgálni, hogy az elektromos rendszer mely részei érzékenyek és azokat a földi szegmenshez hasonlóan Faraday pajzzsal kell körülvenni.

Az akkumulátor és a generátor az egyenáramú tápellátás alapja. A generátor a feszültség szabályozóval stabil feszültségszintet állít elő a belsőégésű motor forgómozgásából, amíg a jármű üzemel. Az áramkör negatív sarka a jármű karosszériájához csatlakozik. Ezek az összetevők immunisnak tekinthetők EMP szempontból.

A gyújtás rendszer (5. ábra) autótól függően lehet sérülékeny vagy ellenálló. A gyújtás vizsgálatakor feltételezzük, hogy a rendszer a modern, a jármű számítógép vezérelt. A régebbi dízelmotorok komputervezérelt üzemanyag-ellátó és gyújtás-rendszer hiányában sokkalta megbízhatóbbak EMP támadás alatt. A szabványos jármű számítógép rendszereinek üzemi feszültsége kevesebb, mint 5V (200mA). Ilyen, a szabvány által szabályozott egység például a motorvezérlő (ECU), váltóvezérlő (TCU), a blokkolásgátló (ABS) és a karosszéria-vezérlő egység (BCM). Továbbá a katonai járművekbe telepített C4I rendszerek rendkívül komplex kialakításúak a beépített rádióval, műholdas kapcsolattal, fegyverirányító rendszerekkel és sok egyébbel, amik érzékenyek az elektromágneses interferenciára és ezáltal EMP sérülékenyek.

A gyújtásrendszer (5. ábra) magas feszültségű elektromos töltést hoz létre, ami a gyújtókábelen keresztül jut a gyújtógyertyákhoz. A töltést a gyújtástekercs hozza létre és a gyújtáselosztóba táplál. A modern járművekben egy számítógép időzíti a hengerenkénti gyújtást, és ez a számítógép több mindenért felelős, úgymint gyújtás-időzítés vagy üzemanyag keverék, de felügyeleti funkciókat is ellát, tehát nyilvánvalóan szüksége van EMP védelemre, Faraday kalitkára. A gyújtástekercs és a gyújtógyertyák immunisnak tekinthetők. A kihívás azonban a számítógép-vezérelt gyújtástekercset a gyertyákkal összekötő 20kV-os vezeték megvédése. Megfelelő szigetelés szükséges a csatlakozók és a gyújtás rendszer komputere közé.

http://www.protectiongroup.com/ProtectionTechnologyGroup/media/PTG/WhitePapersandTechnicalNotes/1474-001.pdf (letöltve:2014.04.15)



5. ábra: Egyszerűsített gyújtás rendszer.[20]

Tehát, míg az akkumulátor és a generátor immunisnak tekinthető EMP szempontból, addig a rádió és a tranzisztor alapú vezérlő rendszer alapvetően sebezhető. Ezek az érzékeny rendszerek általában elszórtan a motortérben, a műszerfal alatt és a csomagtérben helyezkednek el. Minden egyes kritikus alrendszer saját, letestelt Faraday kalitkát igényel, minden csatlakozási pontnál zavarszűrővel, túlfeszültség elleni védelemmel. A vezérlők hálózati eszközökkel kapcsolódó kábeleit zárt árnyékoláson, forrasztva vezethetjük. Minden vezeték-átvezetési és becsatlakozási ponton, vezérlőknél és érzékelőknél gondoskodni kell a zavarvédelemről. A kábeleken külső árnyékoló harisnyát használva nagyban javítható a védelem.

Minden fémes szerkezetet egyetlen test pontra kell kötni. Minden korábban említett Faraday védelmi rendszernek megbonthatatlanul és állandóan a kocsiszekrényhez kell csatlakoznia. Hasonlóan a repülők vagy űrjárművek elektromos rendszeréhez, a karosszéria a gumikerekek szigetelése miatt föld független, relatív test pont. Követve a vezérlő rendszer vezetékeink az útvonalát, Faraday kalitkába kell zárni mindent, a generátort, tápellátás és gyújtás rendszer tranzisztoros áramköreit, komputereit. Végül minden vezeték átvezetési és becsatlakozási ponton gondoskodni kell a zavarvédelemről, hogy semmilyen külső zavarjel ne jusson a rendszerbe, elektromágneses fenyegetés esetén.[21]

[20] *EMP Mitigation. Protecting Land Mobile Vehicles from HEMP Threat Environment http://www.protectiongroup.com/ProtectionTechnologyGroup/media/PTG/WhitePapersandTechnicalNotes/1474-001.pdf (letöltve:2014.04.15)*

[21] *uo.*

Következtetés

A cikk megírásával arra kívántam rámutatni, hogy az űrben működő civil vagy katonai távközlési rendszerek, illetve földi- és felhasználói elemei milyen mértékben védhetők egy esetleges EMP támadás ellen.

A fenti vizsgálat alapján a következő megállapítások tehetők:

1. A műholdas szegmens EMP elleni védelme nem megoldott. Kutatásaim során nem találtam olyan védelmi megoldást, amely megvédené a műholdakat egy esetleges EMP ellen.
2. A földi szegmens van kitéve legjobban az EMP támadásoknak, védelmük a cikkben bemutatott eszköz rendszerrel megoldható.
3. A felhasználói szegmens védelmét a harci járművek adta mobilitás és védelmi képességek alapján a földi szegmenssel azonos kategóriába sorolom.

Az általam megismert szakirodalomból egyértelműen kitűnik, hogy a műholdas kommunikációs rendszerek működésnek biztosítása létkérdés, védelmüket biztosítani kell, azonban meg kell vizsgálni, hogy milyen módszerrel és anyagi ráfordítással. A bemutatott eszközrendszer alkalmas a földi kiszolgáló és felhasználói szféra védelmére, telepítésüket jól kidolgozott nemzetközi és hazai szabványok biztosítják. Az alkalmazott módszerek ismertek, költséghatékonyak és jól alkalmazhatók.

Felhasznált irodalom

1. Options for Military Satellite Communications Debated http://www.spacepolicyonline.com/news/options-for-military-satellite-communications-debated (letöltve: 2014. 01. 11.)
2. Article courtesy of Air Force Space Command and is the combined work of several subject-matter experts. http://www.milsatmagazine.com/story.php?number=1915825642 (letöltve: 2014. 01. 11.)
3. Options for Military Satellite Communications Debated http://www.spacepolicyonline.com/news/options-for-military-satellite-communications-debated (letöltve:2014.04.02)
4. Úton a második AEHF

http://www.urvilag.hu/a_nemzetbiztonsagert/20120505_uton_a_masodik_aehf (letöltve:2014.04.02)
5. http://www.lockheedmartin.com/us/products/advanced-extremely-high-frequency--aehf-.html (letöltve:2014.04.02)
6. Atlas-5 - mindent a biztonságért http://www.mernokbazis.hu/cikkek/atlas-5-mindent-biztonsagert (letöltve:2014.04.03)
7. Oroszország nagy reményeket fűz a kis műholdak kidolgozásához http://hungarian.ruvr.ru/2012_06_14/78139479/ (letöltve:2014.04.03)
8. Pico-és nano-műholdak gazdaságos előállításával kísérleteznek http://www.sat.hu/hirek/pico-es-nano-muholdak-gazdasagos-eloallitasaval-kiserleteznek/1555.html (letöltve:2014.04.03)
9. System Approach to EMP Mitigation http://www.protectiongroup.com/ProtectionTechnologyGroup/media/PTG/WhitePapersandTechnicalNotes/1474-000.pdf (letöltve:2014.04.15)
10. Farkas György: Készülékek zavarvédelme 2008 Győr pp.:1-51 http://www.sze.hu/~farkasgy/EMC-konyv/EMC1.doc (letöltve:2014.04.15)
11. EMP Mitigation. Protecting Land Mobile Vehicles from HEMP Threat Environment http://www.protectiongroup.com/ProtectionTechnologyGroup/media/PTG/WhitePapersandTechnicalNotes/1474-001.pdf (letöltve:2014.04.15)
12. Haig Zsolt-Kovács László: Kritikus infrastruktúrák és kritikus információs infrastruktúrák Tanulmány 2012 Nemzeti Közszolgálati Egyetem pp. 285 http://kovacsx.hu/download/doktorikepzes/KOVASZ_KII_Tanulmany_FINAL.pdf (letöltve: 2014. 05. 04)
13. Todd Harrison: The Future Of Milsatcom 2013 Center for Strategic and Budgetary Assessments.
14. Prof. Dr. Haig Zs.-Prof. Dr. Kovács L.-Dr. Ványa L. Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata, Felderítő Szemle Budapest X. évfolyam 1-2. szám, 2011. március-június, HU ISSN 1588-242X (pp.:183-207)