HADMÉRNÖK

IV. Évfolyam 1. szám - 2009. március

Munk Sándor
Zrínyi Miklós Nemzetvédelmi Egyetem
munk.sandor@zmne.hu

Zsigmond Gyula
Zrínyi Miklós Nemzetvédelmi Egyetem
zsigmond.gyula@zmne.hu

AZ INFORMATIKAI RENDSZEREK BIZTONSÁGÁNAK EGY SAJÁTOS RÉSZTERÜLETE

Absztrakt

A katonai és polgári informatikai rendszerek megbízható üzemeltetése napjaink egyre növekvő jelentőségű kérdése. Jelen publikáció e problémakör egy sajátos részterületével foglalkozik, különös tekintettel az informatikai eszközök által keltett felharmonikusok informatikai rendszerek biztonságát veszélyeztető hatásaira.

Reliable operation of military and civilian IT systems has continually growing importance in our days. Recent publication presents a specific field of this question, with special regard to effects of harmonics generated by IT devices, threatening IT security.

***Kulcsszavak**: informatikai biztonság, fizikai fenyegetés, felharmonikus, mérés, túlterhelés ~ IT security, physical threat, harmonic, measurement, overload.*

Bevezetés

Napjainkban nem kíván különösebb szemléltetést az informatika, a korszerű információtechnológia szerepének növekedése, az informatikai szolgáltatások egyre bővülő, az élet minden területére kiterjedő alkalmazása. Az informatika-alkalmazás a társadalmi, szervezeti és magánéletbeli folyamatok szinte mindegyikét egyre intenzívebben áthatja, ami – a technológiai fejlődés általános törvényszerűségeinek megfelelően – az új lehetőségek mellett új problémák megjelenésével is együtt jár.

Az informatikai rendszerek, eszközök új sebezhetőségeket hordoznak, új veszélyeztetések érvényesüléséhez teremtenek lehetőségeket. A széleskörű alkalmazás kialakulásával a fenyegetettségek elleni védettség, a biztonság szerepe, jelentősége az informatikai rendszerek esetében is folyamatosan nő, amelynek indokoltságát a gyakorlat tapasztalatai nap, mint nap igazolják. Az alábbiakban az informatikai biztonság egy sajátos területével foglalkozunk.

Az informatikai rendszerek biztonságáról

Az „informatikai” jelző értelmezésével a gyakorlatban – sőt még a szakirodalomban is – számos különböző változatban találkozhatunk. Ezért szükségesnek tartjuk rögzíteni, hogy jelen publikációban egyes fogalmak alatt mit értünk.

Informatikai eszköz alatt (a legtágabb értelemben) mindazon technikai eszközöket értjük, amelyek információs tevékenységeket – információszerzés, gyűjtés, továbbítás, tárolás, átalakítás, megjelenítés – támogatnak, vagy valósítanak meg. Ennek az értelmezésnek az indokát az ezen definíció alá sorolható eszközök technológiai alapjainak azonossága és folyamatos konvergenciája, integrációja képezi.

Az előző fogalomra támaszkodva informatikai rendszer alatt informatikai eszközök, programok, adatok, valamint a működtető személyzet információs funkciók, tevékenységek megvalósítására létrehozott rendszerét értjük. Ez a meghatározás így – a szűkebb értelemben vett számítástechnikai rendszerek mellett – magában foglal az információtechnológiai összetevőkre épülő legkülönbözőbb – érzékelő, mérésadatgyűjtő, távközlési, helymeghatározó, azonosító, műsorszóró, folyamatirányítási, stb. – rendszereket is.

Informatikai biztonság alatt jelen publikációban az informatikai szolgáltatások, a szolgáltatott információk és az ezeket biztosító informatikai rendszerek, eszközök olyan állapotát értjük, amelyben ezek az őket érő fenyegetések ellen a megkívánt mértékben védettek [1, 11.o.]. A fenyegetések a felsorolt összetevők bizalmasságát, sértetlenségét, rendelkezésre állását, hitelességét és letagadhatatlanságát veszélyeztetik. A fenyegetéseket, veszélyeztető hatásokat különböző szempontok, – pld. forrásaik, hatásmechanizmusuk – szerint lehet osztályozni. Ennek megfelelően az informatikai biztonság is – különböző nézőpontoknak megfelelően – különböző összetevőkre bontható. Ennek megfelelően találkozhatunk pld. a katonai alkalmazásban is fizikai, személyi, dokumentum-, és elektronikus információbiztonsággal [1, 12.o.]

Legáltalánosabb értelemben a fenyegetések olyan potenciálisan káros, vagy meg nem engedett [kölcsön]hatások, amelyek a védendő objektumot – annak létét, állapotát, működését, vagy valamely tulajdonságát – károsan, egy megengedett/elfogadható mértéknél jobban befolyásolják. A fenyegetést jelentő kölcsönhatások végbemehetnek az adott objektum és környezete között, vagy érvényesülhetnek az objektumon belül, ennek megfelelően beszélhetünk külső, vagy belső fenyegetésekről [1, 5.o.].

A fenyegetések jellegüket tekintve lehetnek egyszerű anyagi kölcsönhatások (fizikai behatás; elektromágneses be-, vagy kisugárzás; radioaktív sugárzás; stb.), lehetnek – egyébként az előbbiek segítségével megvalósuló – információs kölcsönhatások információbevitel, információszerzés, vagy információcsere, valamint az emberi tudatban érvényesülő szellemi kölcsönhatások (pld. megtévesztő propaganda, pánik- vagy félelemkeltés, stb.).

A tapasztalatok azt mutatják, hogy az informatikai biztonsággal kapcsolatban sokszor egy leszűkítő szemléletmód érvényesül. Kiemelt – vagy kizárólagos – szerepet kapnak az információs kölcsönhatások és az ellenük való védekezés eszközei (hozzáférés-védelem, jogosultsági rendszerek, rosszindulatú programok elleni védekezés, stb.). Háttérbe szorulnak viszont a személyi és a fizikai védelem megoldásai. Éppen az empirikus adatok bizonyítják azonban, hogy a tényleges biztonsági események nagy része e két utóbbi területen (vagy ezeken is) jelentkezik [2, 25.o.]. Emiatt mérvadó tudományos és szakmai körökben ma már uralkodónak tekinthető az informatikai biztonság átfogó értelmezése, megközelítése.

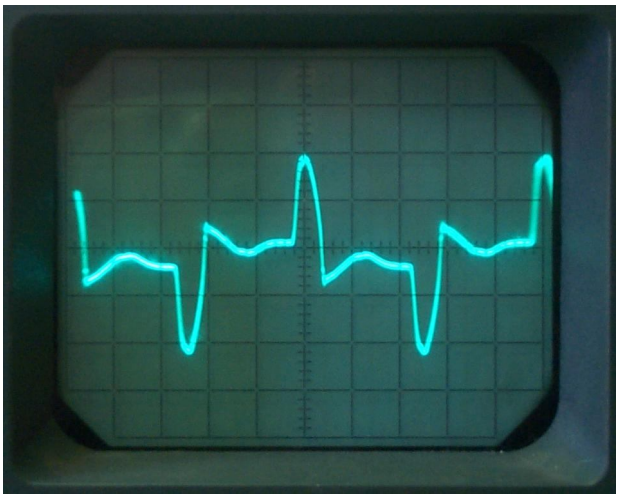
Fizikai biztonság alatt – az informatikai biztonság vonatkozásában – az informatikai rendszer összetevőinek a fizikai (anyagi) támadásokkal, veszélyeztető hatásokkal, jogosulatlan hozzáférésekkel szembeni védettségét értjük [3, 167.o.]. A fizikai hatások, veszélyeztetések kiváltói lehetnek szándékosan rosszindulatúan, vagy gondatlanul tevékenykedő emberek; természeti, vagy ipari katasztrófák, balesetek; valamint az informatikai rendszerek működési

feltételeit biztosító rendszerek. Ez utóbbiak között fontos szerepet kaphatnak az informatikai rendszerek energiaellátását közvetlenül biztosító 0.4 kV-os energiaellátó rendszerek.

Az informatikai rendszerek energiaellátását biztosító villamos energiaellátó rendszerek működési zavarait – az EMC [5, 16-21. o.; 6, 56-61 o.] problémákon kívül – elsősorban a villamos energia minőségét meghatározó összetevőkkel [5, 5-10. o.] kapcsolatos feltételrendszer teljesítésének hiányosságai okozzák. A különböző üzemzavarok megszakíthatják, zavarhatják az információk feldolgozását, továbbítását, hozzájárulhatnak tárolt adatok véletlenszerű módosulásához, elvesztéséhez, sőt eredményezhetik technikai összetevők, részegységek, áramköri elemek meghibásodását, tönkremenetelét is.

Felharmonikusok hatásairól

A továbbiakban a – személyi számítógépek által létrehozott – felharmonikusok [4, 483-487. o.] két olyan hatásával foglalkozunk, amelyek veszélyeztethetik az informatikai rendszerek energiaellátását biztosító 0.4 kV-os hálózatok megbízható üzemét. Egy személyi számítógép által felvett, a felharmonikusok által eltorzított áram hullámalakját lásd az 1. ábrán) [7, 25-30. o.].



1. ábra. Személyi számítógép által felvett áram hullámalakja

a.) Mérési hibák

A felharmonikusok által okozott zavarok egy részét csak méréssel lehet igazolni. Ez különösen vonatkozik a rendszerek azon csoportjára, melyeknél utólagosan – általában korszerűsítés miatt – kerültek beüzemelésre nagy számban személyi számítógépek. Sajnos a rendszer kisfeszültségű megtáplálásánál ezeket a méréseket sokszor nem megfelelő körültekintéssel végzik el. Erre tipikus példa az áram effektív értékének helytelen meghatározása. A továbbiakban ezzel foglalkozunk.

Mint ismeretes a periodikus áram egyik fontos paraméter a k_f formatényező, amely az alábbiak szerint van értelmezve

$$k_f = \frac{I}{I_a} \qquad (1)$$

ahol

I az effektív érték ($I^2=\frac{1}{T}\int_0^T i^2 dt$)

I_a az abszolút középérték ($I_a=\frac{1}{T}\int_0^T |i| dt$)

Szinuszos áram estén

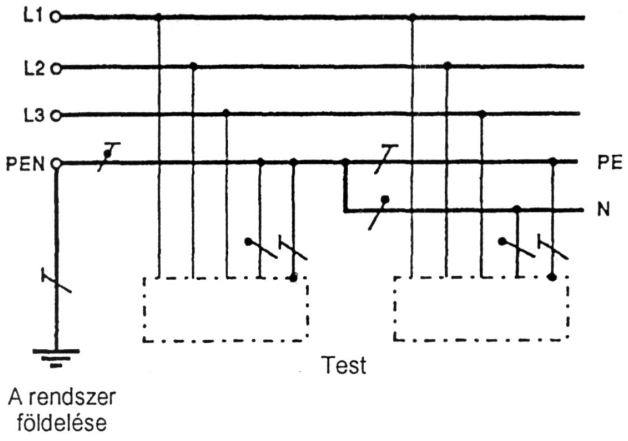
$$k_f=\frac{I}{I_a}=\frac{\pi}{2\sqrt{2}}=1{,}11 \qquad (2)$$

Az (2) alapján belátható, hogy szinuszos áram esetén az effektív értéket megkapjuk, ha az abszolút középértéket megszorozzuk („felskálázzuk") a formatényezővel, azaz 1.11-el. Ez az effektív értékre skálázott Deprez rendszerű mérés elve (mint ismeretes a Deprez-műszer váltakozó áramú állásában a mért áram egy kétoldalas egyenirányítón folyik keresztül és így a műszer az abszolút középértéket érzékeli). Ezt a módszert alkalmazzák az analóg műszereknél, de sok „digitális multiméternél" is. Felharmonikusokat is tartalmazó áram esetén az ismertetett mérési módszer a megváltozott értékű formatényező miatt, nem ad valós eredményt. A jelenség vizsgálatához összeállítottunk egy mérést, amelynek segítségével meghatároztuk egy személyi számítógép által felvett áramalakot (lásd az 1. ábrát). Ugyanakkor megmértük – a felharmonikusok miatt a szinusz hullámtól láthatóan nagymértékben eltérő – áram effektív értékét egy Deprez rendszerű multiméterrel, és egy igényes – a piacon kapható – valóságos effektív értéket mutató műszerrel. A multiméter – a megnövekedett formatényező miatt – kb. 40%-al kevesebb értéket mutatott.

A kisfeszültségű energiaellátó rendszer esetében a hibás mérésnek komoly következményei lehetnek, hiszen a megfelelő villamos készülékek, kábelek alkalmazásának egyik fontos korlátázó tényezője az effektív áram által létrehozott melegedés. További probléma, hogy a védelmi elemek kioldási karakterisztikái az áram effektív értékétől függenek, így a nem kívánt kikapcsolások miatt kerülhet az informatikai rendszer zavarállapotába. Ezért az olyan kisfeszültségű rendszereknél ahol személyi számítógépek utólagos telepítésére kerül sor – a terhelhetőség megállapítására – Deprez rendszerű műszerek helyett, a valóságos effektív értékeket mérő – viszonylag könnyen beszerezhető – műszerekkel kell az ellenőrző méréseket végrehajtani.

b.) Nullavezető túlterhelése

Magyarországon a 0,4 kV-os rendszerekben a TN rendszerek (hazánkban ma is általánosan használt elnevezéssel: nullázott rendszer) használata terjedt el. Ezeknek az egyik pontja közvetlenül földelt, a villamos berendezések teste ehhez a ponthoz csatlakozik a védővezetőkkel. A TN-rendszereknek különböző típusai vannak, ezek közül a legelterjedtebb TN-C-S-rendszer (lásd 3. ábrát). Ebben a rendszerben külön védővezető van, a nulla- és a védővezető a rendszer egy részében közös [6, 16. o.]. A transzformátor szekunder oldalától indul a három fázisvezeték (L1, L2, L3) és a szekunder oldal földelt csillagpontjából indul a PEN vezeték. Az informatikai rendszerek táplálására gyakorlatilag mindig TN-C-S rendszereket használnak

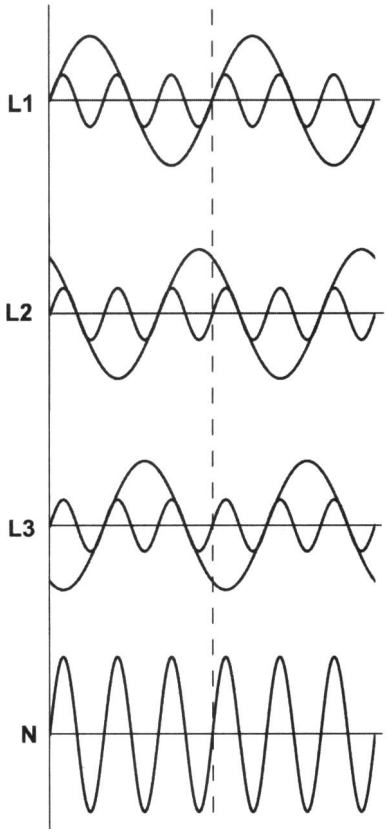


A jelölések az IEC 617-11:1983 alapján	
	Nullavezető (N)
	Védővezető (PE)
	Védő- és nullavezető (PEN)

3.ábra.T-C-S rendszer

Lineáris terhelés esetén az energiaellátó rendszer nullavezetőjén nem folyik nagyobb áram, mint a fázisáram. Másképpen kifejezve szinuszos áramok esetén a nullavezetőben elvileg nem lehet nagyobb áramerősség, mint a fázisvezetékben. Más a helyzet a nullavezető terhelése szempontjából a felharmonikusokat tartalmazó energiaellátó rendszerek esetén. A számítógépek által létrehozott fázisáramok közül a 3-al osztható rendszámú – ún. zérus sorrendű – felharmonikusok [7, 29.o.] az üzemeltetés során komoly gondokat okozhatnak. Ugyanis ezek az áramok — ellentétben az alapharmonikus, valamint a pozitív és negatív sorrendű felharmonikus áramokkal — a kisfeszültségű energiaellátó rendszer nullavezetőjében összeadódnak (lásd 3.ábra). Ennek következtében a nullavezető (N) árama a megfelelő fázisvezetők (L1, L2, L3) áramainál jóval nagyobb lehet, azaz a nullavezető túlterhelődhet.

A jelenleg üzemelő rendszerek kisfeszültségű energiaellátásának tervezése, a felhasznált kábelek szerkezetének kialakítása olyan szabványok szerint történt meg, amelyek nem vették figyelembe a felharmonikusok nem kívánt hatásait, így a nullavezető az informatikai rendszereket tápláló 0.4 kV-os energiaellátó rendszerekben a fázisvezetőkkel azonos keresztmetszetű, azaz azonos mértékben terhelhető.



3.ábra. Harmadik harmonikus áramok a nullavezetőben

Ebből következik, hogy az ilyen rendszerekről megtáplált számítógépek (a kábelek túlmelegedése miatt) könnyen zavarforrásként fejthetik ki hatásukat, ezáltal veszélyeztetik az informatikai rendszer biztonságát, ezért abban az esetben, ha egy informatikai rendszer fejlesztése során a számítógépek száma nő, az energiaellátó rendszerek megbízható üzem feltételeit ilyen szempontból is mindenképpen ellenőrizni kell.

Összefoglalás

A cikk az informatikai rendszerek biztonságának néhány kérdésével foglalkozik. A kapcsolódó fogalmak pontosítása után, ismertetésre került a személyi számítógépek által keltett felharmonikusok megbízható üzemvitelt veszélyeztető két fontos hatása. A személyi számítógépek az informatikai rendszerek fontos elemei, amelyeknek száma a rendszeren belül változhat. Ebben az esetben – az adott informatikai rendszer energiaellátó rendszerének jellegétől függően – ajánlatos a javasolt vizsgálatokat elvégezni.

Felhasznált irodalom

[1] MUNK Sándor: Információbiztonság vs. informatikai biztonság. – *Robothadviselés 7 tudományos szakmai konferencia anyaga (2007.11.27.), Hadmérnök különszám.*

[2] *2007 Global Security Survey. The shifting security paradigm.* – Deloitte Touche Tohmatsu, London, 2007.

[3] *NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook.* – National Institute for Standards and Technology, Gaithersburg, 1997.

[4] MOHAN, N. – UNDELAND, T.M. – ROBBINS, W. P.: *Power Electronics.* – John Wiley, 2003.

[5] REJTŐ Ferenc: *EMC alapok.* – MEE kiadvány, 2006.

[6] ZSIGMOND Gyula: *Villamos rendszerek tervezésének néhány kérdése I. Egyetemi segédlet.* – ZMNE, 2007.

[7] ZSIGMOND Gyula: *Fejezetek az elektrotechnikából. Egyetemi jegyzet.* – ZMNE, 2007.