A kritikus információs infrastruktúrák védelmének aktuális kérdései témakörben :

Informatikai rendszerek kiesésének és gyors leállításának problematikája, valamint a megtehető költséghatékony intézkedések.

TARTALOMJEGYZÉK

ESETTANULMÁNYOK:

Informatikai rendszerek kiesésének és gyors leállításának problematikája – az ISMS[1] a TIA 942 és az ITIL szemszögéből – és a megtehető költséghatékony intézkedések.

A **II. EU-USA Kritikus Infrastruktúra Védelmi Találkozó** [2] kapcsán a **nap és az űridőjárás felismert veszélyei** alapján bennem felmerült informatika védelmi gondolataim jelen tanulmányom tárgya.

Mondanivalómat elsősorban nem szakembereknek írtam. Megpróbáltam ahol lehetett, **népszerűsítő formában**, mellőzve a tudományos levezetést – de lábjegyzetben utalva ezen, források elérhetőségére – inkább informatikai ismeretek nélkül is megérthető módon megfogalmazni, ezért a megértéshez szükséges minimális ismereteket is tárgyalom. Az volt a szándékom, hogy ilyen tanulmányt írjak. Az olvasónak kell eldönteni, hogy sikerrel jártam-e.

> **Célom, hogy gyakorló szakemberként - lehetőleg nem szakemberek számára is érthető módon - olyan kritikus infrastruktúra védelmi eljárásokra, lehetőségekre hívjam fel a figyelmet és tegyek javaslatokat, amelyek a napi életben alkalmazhatóak és alacsony költségkihatásúak, ugyanakkor alkalmazásukkal nagy a megmenthető IT[3] érték.**

[1] ISMS – Information Security Management Systems – Az ISO 27000 szabvány által leírt, speciálisan az informatikai rendszerek adat és működési biztonságára kialakított minőségbiztosítási és minőségirányítási rendszer.

[2] 2011. június 9.-10.-én Budapesten megrendezett szakértői találkozó.

[3] Információ Technológia – Ebbe a körbe értem mindazokat az infrastrukturális rendszereket, eszközöket és adatállományokat, amelyek elektronikus adatok formájában jelennek meg, ill. ilyen adatfeldolgozást, adat-továbbítást vagy tárolást végeznek.

Vezetői összefoglaló:

1/ Hálózatos informatikai rendszerek veszélyeztetettsége:

1.1/ Az ellátó elektromos hálózat kiesése

1.2/ Az IT hálózat (LAN, WAN, INTERNET) kiesése

1.3/ Az üzemeltető rendszerek (hűtés, klíma) kiesése

1.4/ Üzemelő IT hardver és a Hálózat sérülései

1.5/ Üzemelő szoftver és adatállományok sérülései

2/ A II. EU-USA Kritikus Infrastruktúra Védelmi Találkozó [4] kapcsán felmerült informatika védelmi kockázatok szempontjából vannak megtehető költséghatékony intézkedések.

2.1/ Az IT rendszer kiesése szempontjából elsődleges az okozható értékszemléletű kár modell, és megelőzési költség függvény megállapítása, azaz a keletkezhető kár üzleti érték, vagy eszmei (irracionális) érték alapú.

2.2/Ennek folyománya a megelőzésre fordítható költségkeret kijelölése.

3/ A megtehető költségtakarékos intézkedések:

3.1/ ISMS megelőző intézkedései
3.2/ Operatív megelőző intézkedések
3.3/ Operatív, más szervezési alapon álló áthidaló intézkedések
3.4/ Vészhelyzeti intézkedés
3.5/ Helyreállítási intézkedés

4/ Ezeken felüli – globális – összeomlás esetén, az erőforrásokat az új rendszerek felépítésére célszerű fordítani. Ennek beruházói igény összefoglalásban fel kell használni az összeomlott rendszer kapcsán szerzett tapasztalatokat.

5/ Négy esettanulmány alapján kidolgozott részletes javaslatok a tanulmány 82. oldalától olvashatók.

[4] 2011. június 9.-10.-én Budapesten megrendezett szakértői találkozó.

Bevezető téma összefoglaló:

A téma és címválasztás alátámasztására ismertetem az alapvető **kritikus infrastruktúra definíciót**, majd népszerűsítő formában ismertetem a hálózatos **rendszerek alapvető ismereteit** és az **összeomlásukkal foglalkozó elméletek**et.

Ezt követően felvázolom az eddig kidolgozatlan – az adatállományok és informatikai **rendszerek értékének** felbecslése – (javasolt) önálló kutatási témát és melynek kapcsán bemutatok, két általam kidolgozott érdekes döntési modellt.

Majd az **ISMS**-hez (**I**nformation **S**ecurity **M**anagement **S**ystems, az **ISO 27000**:2006 – az információbiztonság irányító rendszereihez) kapcsolódó olyan megtehető intézkedéseket tárgyalok, amelyek alacsony költségkihatásúak, ugyanakkor alkalmazásukkal nagynak vélem a megmenthető IT értéket.

Az **ISO 27000**[5] (**ISMS**) mellett röviden ismertetni fogom a vállalati informatikai központok és az adat központok **TIA 942**[6] szabvány szerinti besorolását. Ismertetni fogom ennek **ITIL**[7] szerződéskötési ajánláshoz kapcsolódását. Ezt követően kitérek **négy esettanulmányban**, egyrészt két általam megvalósított **ERP**[8] vállalatirányítási rendszer rövid bemutatására, illetve részvételemmel egy banki és egy újépítésű datacenter projekt kapcsán felmerült tapasztalatokra. Ahol lehetett ismertettem a jellegzetes sérülékenységet (tapasztalatokat), majd elsősorban az ISMS/ISO 27000:2006 alapján, és a TIER klasszifikáció alapján olyan általánosan megtehető intézkedéseket mutatok be, amelyek alacsony költségkihatásúak, ugyanakkor alkalmazásukkal nagy a megmenthető érték.

Végül megnézzük, miért is beszéltünk ennyit minderről.

A fentiek szükségessége szempontjából röviden ismertetem az **űridőjárás és a naptevékenység** kapcsán jelenleg ismert NASA és ESA (Amerikai és Európai Űr Ügynökség) új információkat és kitérek a már megismert földi veszélyekre is. Legvégül összefoglalom a tárgyban tett javaslataimat.

---

[5] A Nemzetközi Szabványügyi Szervezet (International Organization for Standardization) szabványa. Speciálisan az informatikai rendszerek adat és működési biztonságára kialakított minőségbiztosítási és minőségirányítási rendszer.

[6] Telecommunications Industry Association – az USA és Kanada Telekommunikációs Ipartestületei által közösen az Amerikai Nemzeti Szabványügyi Intézettel (ANSI) összhangban kiadott szabvány az adatközpontok biztonsági szintjeinek meghatározásához és besorolására: un.: TIER 1-2-3-4 fokoztok.

[7] ITIL: Information Technology Infrastructure Library: Nemzetközileg elfogadott szerződéskötési ajánlás, amelyet speciálisan az informatikai szerződések és projektek lebonyolítására alakítottak ki.

[8] Enterprise Resource Planning. – Integrált szoftver, amely a vállalatirányítás és vállalati működés üzleti folyamatainak követésére és tervezésére képes.

Mi a kritikus infrastruktúra?

A Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság definíciója szerint:
„Kritikus infrastruktúra általános fogalma,[9] *azaz egy országon belül a lakosság szellemi és tárgyi életfeltételeit megteremtő, a gazdaság működését elősegítő vagy lehetővé tévő azon szervezetek, létesítmények, létesítményrendszerek, hálózatok összessége vagy ezek részei, amelyek megsemmisülése, szolgáltatásaik vagy elérhetőségük csökkenése egy adott felhasználói kör létére, lét- és működési feltételeire negatív hatással jár.*

A fenti fogalmat az alábbi 5 alapvető tulajdonság teszi teljessé:

- ***interdependencia*** *– egymástól való függőség;*
- ***informatikai biztonság*** *– kiemelt terület, informatizált munkafolyamatok;*
- ***üzemeltetés*** *– sajátosságok, egyedi jelleg;*
- ***dominó-elv*** *– láncreakció-szerű sérülés/károsodás;*
- ***leggyengébb láncszem*** *& rész-egész elv – összekapcsolódó hálózatok stabilitása a leggyengébb elem erősségétől függ.*”

Világunkban az alapvető állami és gazdasági működések informatikán, elektronikus távközlésen és globális rendszereken alapszanak ezért az informatikai rendszerek védelme, (mint kiemelt terület) lényeges és meghatározó új szegmense a kritikus infrastruktúrák védelmének és ezen belül rendelkezik a fenti fogalom öt alapvető tulajdonságával.

Az informatikai rendszereket együttesen jellemzi az IT alapú munkafolyamatok léte, ezek egymástól való függősége, az üzemeltetés sajátosságai valamint a „leggyengébb láncszem” szakadása esetén a dominó-elvszerű meghibásodás eszkaláció, a rendszer összeomlása.

Nagyon kevés olyan alapvető infrastruktúra van mai világunkban, amelynek ne lenne lényeges informatika függősége.

[9] Forrás:BM OKF
http://www.katasztrofavedelem.hu/index2.php?pageid=lakossagvedelem_kritikus_infrastruktura

Az egymástól való függőség - a hálózati topológia:

Rendszerszemléletű megközelítésben a gráfok matematikai[10] leírásán keresztül vizsgálhatjuk az informatikai rendszereket, amelyek érdekes következtetésre vezetnek az **ISMS**[11] szempontjából. A **hálózati topológiának**[12] nevezett fogalomkör, amely az informatikában meghatározza a számítógépek egymáshoz kapcsolódását és az ezek közötti adattovábbítást jelenti. Ezen keresztül vizsgáljuk a rendszer egyes elemének kiesése által okozott tovagyűrűző hatásokat.

Mi is az a hálózati topológia?
Anélkül, hogy tudományos részletességgel ismertetném a mai korszerű hálózatok és adatátviteli technikák mélységeit, inkább egyszerűen szeretném (felhasználói szempontból) bemutatni a működést és annak korlátait.

Az internet világában a hálózatra kapcsolódó eszközöket és a hozzájuk köthető biztonsági fokozatokat az alábbi elméleti nagy csoportokra lehet bontani:

1- saját (önálló fizikai adat) kapcsolattal rendelkező hálózatok
2- internet (vagy más közösségi hálózaton működő) alapú egyenrangú hálózatok
3- internet (vagy más közösségi) alapú, de elkülönült „dedikált” hálózatok

Itt tegyünk egy kis elméleti kitérőt. Nagyon kicsit. Nagyon zanzásítva…

Ha anyósunknak akarunk levelet küldeni, a lehető legegyszerűbb megoldás, ha megírjuk levelünket és elballagunk vele, átadjuk. (Ez esetben nagy valószínűséggel találkoznunk is a címzettel.)

Az elvitt egy darab levél terjedelmét nézve, jó sok információt tudunk egy levél (adat **csomag**[13]) átadásával, a kedves mamával ekként közölni. Attól

[10] Frank András, ELTE TTK. 2011 Operációkutatás egyetemi jegyzet
[11] ISMS – Information Security Management Systems – Az ISO 27000 szabvány által leírt, speciálisan az informatikai rendszerek adat és működési biztonságára kialakított minőségbiztosítási és minőségirányítási rendszer. A rendszerkövetelményeket az ISO 27001:2006 írja le.
[12] Andrew S. Tannenbaum, Prentince Hall – PANEM 1999 Computer Networks. Third edition.
[13] Andrew S. Tannenbaum, Prentince Hall – PANEM 1999 Computer Networks. Third edition 25. oldal

függően, hogy milyen gyorsan ballagva jutunk el az anyósék házához, beszélhetünk az **átvitel sebességéről**.[14] Ha lusták vagyunk, és mindenképpen kerülnék a személyes találkozást úgy levelünket postagalambra is bízhatjuk, de így már csak kisebb (rövidebb) levelet tudunk küldeni, de lényegesen hamarabb odaér – nagyobb az átviteli sebesség, ha a macska nem kapja el a postagalambunkat, ami jelen esetben **átviteli hiba, adatvesztés**[15] lenne.

Tovább egyszerűsítve, ha másra bízzuk a levelünket kézbesíteni, akkor arra **címzés**t[16] is kell írni. Kinek akarjuk továbbíttatni. A galamb persze fejből tudja a címet, hiszen hazarepül. Végül – és ez már a kézbesítő feladata – valamilyen **útvonal**on[16] el kell juttatni a címhez.

Tehát ismétlem, végletesen leegyszerűsítve: adattovábbításnál a hálózaton először kiválasztjuk, az un. **fizikai réteget** [17] azaz, hogy mi viszi az információt, amely egyben meghatározza, hogy milyen **sávszélességgel**[18] mekkora adatátviteli sebességet tudunk elérni. Az **adatkapcsolati réteg**[12] felel többek között az információnak a fizikai rétegben az A pontból B pontba „címzés” juttatásáért. Végül többek között az un. **hálózati réteg**[12] biztosítja, hogy lesz egy megfelelő **útvonal**[19] az információ célba érkezéséhez.

[14] Andrew S. Tannenbaum, Prentince Hall – PANEM 1999 Computer Networks. Third edition 104. oldalon a 2.1.3 cím: A csatorna maximális adatátviteli sebessége.

[15] Andrew S. Tannenbaum, Prentince Hall – PANEM 1999 Computer Networks. Third edition, 212. oldalon 3.2 fejezet: Hibajelzés és javítás

[16] Andrew S. Tannenbaum, Prentince Hall – PANEM 1999 Computer Networks. Third edition, 457. oldalon. Valamint:
Forrás: Novosel-Hudson-Stewart/Kiskapu kiadó 2000. TCP/IP 293. oldaltól.

[17] Andrew S. Tannenbaum, Prentince Hall – PANEM 1999 Computer Networks. Third edition.
2. fejezet „A fizikai réteg” 3. fejezet „Az adatkapcsolati réteg” 5. fejezet „A hálózati réteg”

[18] Andrew S. Tannenbaum, Prentince Hall – PANEM 1999 Computer Networks. Third edition.
2. fejezet 2.2.4 a 108. oldalon

[19] Andrew S. Tannenbaum, Prentince Hall – PANEM 1999 Computer Networks. Third edition. 247-257. oldalakon tárgyalja a gráfelméleti megközelítést. A 251. oldal tetején mondja ki a választható útvonalak tekintetében – nem továbbítható egy üzenet: Ha nincs a részhalmazból kivezető átmenet, vagy nincs olyan átmenet a részhalmazban, amely továbblépést eredményez.

Vegyünk két egyszerűsített példát táblázatban[20] a szemléletesség kedvéért:

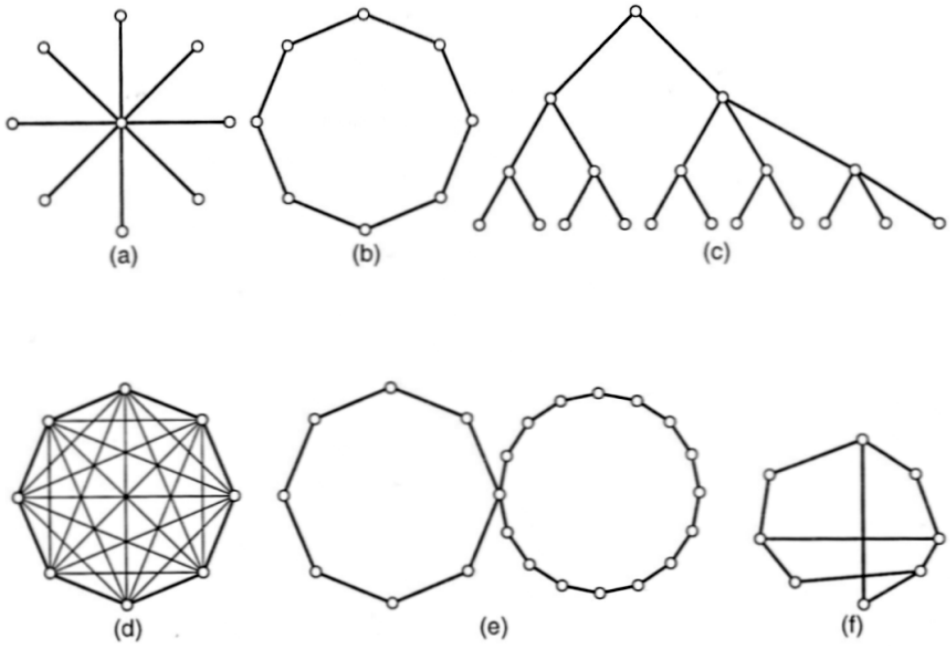
Fizikai réteg: (mi viszi az információt)	Levél és postagalamb	Email
Adatkapcsolati réteg: (hogyan biztosítom, hogy az információ A-ból B-be jusson)	Rákötöm a lábára haza röpül (nyugtázatlan, összeköttetés nélküli szolgáltatás)	Például: Point-to-Point Protokoll
Hálózati réteg: (milyen útvonalon biztosítom az információ továbbítását)	Toronyiránt röpül	Hálózati topológia

[20] Forrás: A Szerző által összeállított ábra.

Hogyan dől össze egy hálózati topológia?
(Miért, összedől?)

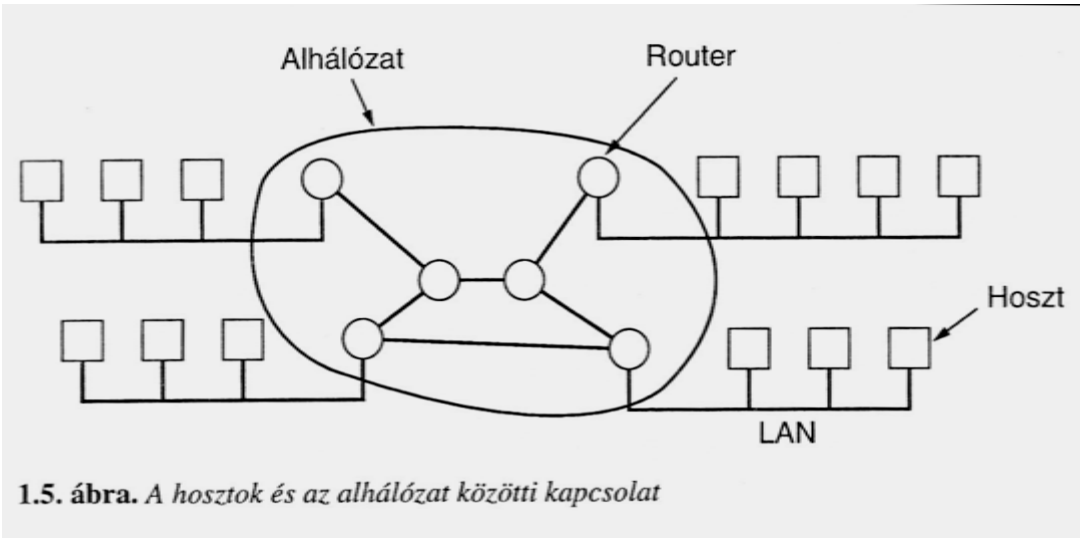
Hálózati topológia[21] alatt az egymással összeköttetésben lévő, egymással kommunikálni képes informatikai eszközöket értjük.

Egyszerű gráfos megjelenítésben így néz ki:



1.6. ábra. *Néhány lehetséges két pont közötti alhálózati topológia. (a) Csillag. (b) Gyűrű. (c) Fa. (d) Teljesen összekötött. (e) Egymást metsző gyűrűk. (f) Szabálytalan*

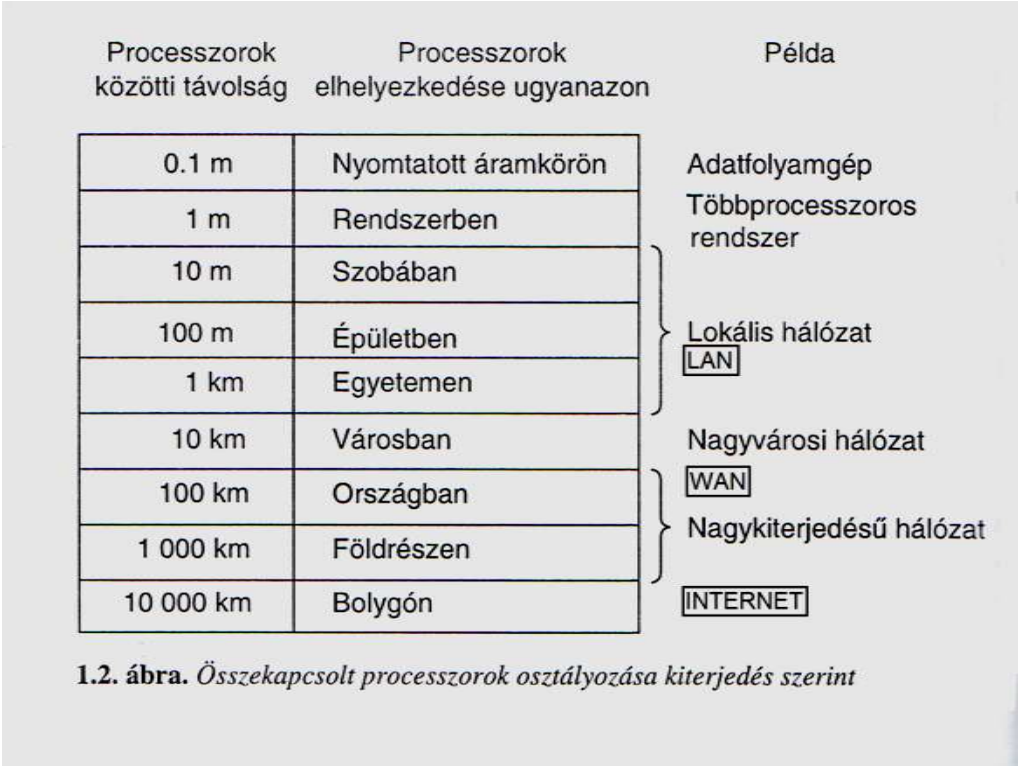
Informatikai megoldásként rögzítve ilyen is lehet:



1.5. ábra. *A hosztok és az alhálózat közötti kapcsolat*

[21] Andrew S. Tannenbaum, Prentince Hall – PANEM 1999 Computer Networks. Third edition. 30.-31. oldal

A hálózatok klasszifikációját, azaz rendszertanilag milyen hálózatokat különböztetünk meg az alábbi összefoglaló ábra szemlélteti.[22]



Processzorok közötti távolság	Processzorok elhelyezkedése ugyanazon	Példa
0.1 m	Nyomtatott áramkörön	Adatfolyamgép
1 m	Rendszerben	Többprocesszoros rendszer
10 m	Szobában	
100 m	Épületben	Lokális hálózat LAN
1 km	Egyetemen	
10 km	Városban	Nagyvárosi hálózat WAN
100 km	Országban	Nagykiterjedésű hálózat
1 000 km	Földrészen	
10 000 km	Bolygón	INTERNET

1.2. ábra. *Összekapcsolt processzorok osztályozása kiterjedés szerint*

A korábbi években a számítógép hálózatokat leíró matematikai modellek, azon a feltevésen alapultak, hogy ha egy számítógépről elküldünk egy adatcsomagot egy címre, akkor az elvileg a világ informatikai hálózatán szinte bárhol járva juthat el a címzetthez és… úgy vélték a világháló nem tud összeomlani.

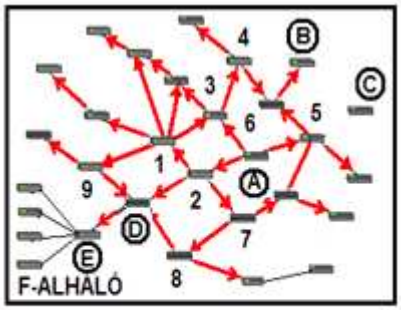
Ennek az alapja az, hogy az adatcsomag a címhez való eljuttatást a hálózati réteg biztosítja, amely működése elvileg úgy írható le, hogy minden adattovábbító pont ismeri a szomszédos adattovábbító pontokat és azokat „végigkérdezve” informálódik ismerik-e, fenti érdekes példánknál maradva: a kedves mama címét, de legalább a felé vezető irányt.

Ezt a körbekérdezést hívjuk **broadcast[23] -nak,** amely ha sikerrel zárul tehát jelentkezik legalább egy továbbító, aki ismeri a címzett felé vezető utat, akkor az adatcsomag elindul a maga igazolt következő továbbítójához.
A matematikusok úgy vélték, hogy ez a kapcsolati hálón, hullámszerűen végigfutó permanens ismétlődő körbekérdezés biztosítja, hogy a világháló

[22] Forrás: Andrew S. Tannenbaum, Prentince Hall – PANEM 1999 Computer Networks. Third edition. 26. oldal, jellegzetesen az ETHERNET (10BASE5, 10BASE2) hálózatok használják.(Kivéve 10BASE-T)
[23] Forrás: Novosel-Hudson-Stewart/Kiskapu kiadó 2000. TCP/IP 24. oldal

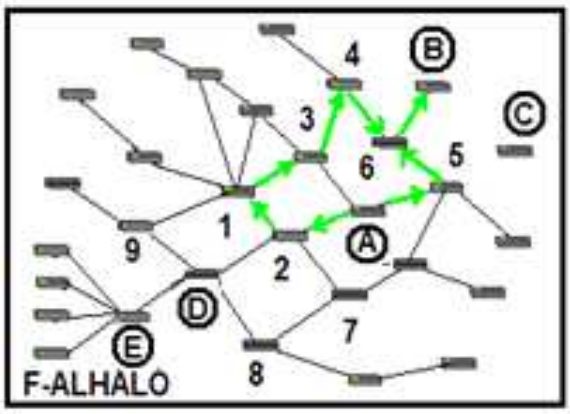
nem tud összeomlani, mert létező címek között mindig lesz egy járható irány amerre az adat továbbhaladhat.

A technika fejlődésével ez a „körbekérdezés” finomodott, mert nagyon sok időt emészt fel mindig a „szomszédjainkkal trécselni” ki ismer útvonalat levelünknek. Létrejöttek olyan meghatározott irányokba továbbító rendszerek, melyek, vagy csak egy **unicast**[24] meghatározott irányba küldenek tovább adatokat, vagy néhány **multicast**[25] meghatározott kapcsolatuk van.
A három szemléltető ábrából[26] az első:

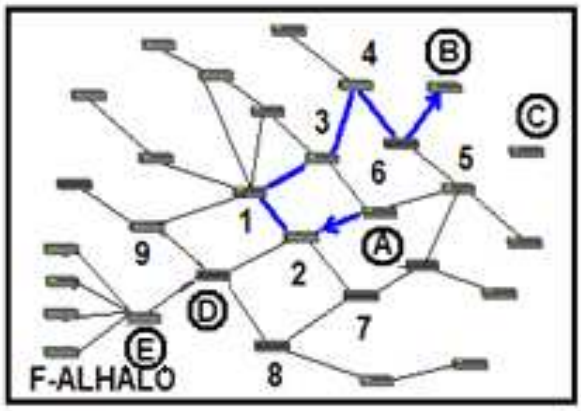


BROADCAST
Létező A-B között mindig van egy létező útvonal.

A lényeg az lényeg maradt, a mai legkorszerűbb hálózati rendszerekben is van broadcast, legfeljebb **uni-** vagy **multicast** továbbítja.



MULTICAST
Létező A-B között több meghatározott útvonal van.



UNICAST
Létező A-B között egy meghatározott útvonal van.

A legrégibb, és amivel a legtöbb probléma volt – ezért mára visszaszorult – az un. **HUB**[27]. A passzív HUB amely a leginkább sérülékeny hálózati

[24] Forrás: Andrew S. Tannenbaum, Prentince Hall – PANEM 1999 Computer Networks. Third edition
[25] Forrás: Andrew S. Tannenbaum, Prentince Hall – PANEM 1999 Computer Networks. Third edition
[26] Forrás: Internetes forrásból származó rajznak, a Szerző által jelen mondanivalóhoz lényegesen módosított és tanulmány tartalmával kiegészített ábrái.
[27] HUB: Csillagtopológiájú számítógép hálózat kapcsoló eleme. Lásd: jelen tanulmány 6. oldal 1.6-os ábra a) pontja. Jellegzetesen passzív elem, és a szomszédos pontok kapcsán folyamatosan minden

adattúlterhelés szempontjából. A HUB minden irányban, válogatás nélkül brodacastol aminek a folyománya, hogy minél több a kapcsolati hiba, annál több a kapcsolat felvételi kísérlet és ebből keletkező további kapcsolati hiba és ez – az ördögi kör – végül a hálózati tényleges adatforgalom leállásához vezet. Amiért mégis meg kell említeni, az a SATELIT rendszerek, különösen, amelyek még a 80'-as évek végén, a 90'-es évek elején lettek földkörüli pályára állítva és még ilyen technológiát is alkalmaznak. A **switch -ek**[28] is boldogan kérdezgetnek és a **router -ek**[29] pedig **IP cím** [30]alapján még azt is **vizsgálják**[31], merre küldhetik tovább a beérkezett üzeneteket és a különféle internet **címszervereket**[32] is kérdezgetnek. Ezen esetekben is számos útvonal lehetséges, amelyek egymással konkurálnak.

Olyan ez, mintha levelünket rábíznák valakire, [33] aki megy a kedves mama felé, és bár nem hozzá megy, de feléje és az a valaki végigkérdezi az ismerőseit a környéken, hogy ki mindenki ismeri a kedves mama címét, vagy legalább annak irányát majd egynek beadja a levelet, aki azt állítja, magáról tudja, merre kell továbbítania a levelet és végül lesz majd egy, aki átadja a kedves mamának.

A matematikusoknak igazuk lett, tetszőleges hálózaton, két létező cím között elvileg mindig lesz egy választható útvonal. Azonban a

irányba küld kapcsolattartó adatokat (Broadcast) ennek eredményeként hálózati zavarok esetén könnyen túlterhelhető és ezáltal, megáll az adatforgalom.

[28] Switch: Aktív jelerősítést is tartalmazó adatforgalmi eszköz, amely a hozzákapcsolt számítógépek közötti adatforgalmat címzés és az adatcsomag épsége szerint is vizsgálja, hibás adatcsomagokat nem küld tovább, ezzel elkerüli a hálózat túlterhelését illetve lelassulását.

Forrás: Reynders-Wrigth/Kiskapu kiadó 2005. TCP/IP és ETHERNET hálózatok a gyakorlatban

[29] Router: Aktív adatforgalmi eszköz, amely a hozzákapcsolt számítógépek és a szerverek IP címtára alapján az adatforgalmat már csak az adatcsomag címzése szerint meghatározott IP cím irányokba küldi tovább. Lassabb kommunikációt, de nagy rendszerek esetén biztonságosabb adattovábbítást tesz lehetővé. Feladatuk, hogy adat csomagokat küldjenek egyik hálózatból a másikba.

Forrás: Reynders-Wrigth/Kiskapu kiadó 2005. TCP/IP és ETHERNET hálózatok a gyakorlatban

Forrás: Novosel-Hudson-Stewart/Kiskapu kiadó 2000. TCP/IP 25. oldal

[30] IP cím: Internet Protokoll cím: Egyedi hálózati azonosító szám, amely a TCP/IP Internet Protokollt használó hálózatokban ezzel a számmal (például: 10.1.21.112) azonosítja a kapcsolódó gépeket és a broadcast címmel (alhálózati maszk) (például: 255.255.255.0) azonosítja a tovább küldési irányt.

Forrás: Novosel-Hudson-Stewart/Kiskapu kiadó 2000. TCP/IP 393. oldal

[31] Forrás: Novosel-Hudson-Stewart/Kiskapu kiadó 2000. TCP/IP 71. oldal.

Forrás: Reynders-Wrigth/Kiskapu kiadó 2005. TCP/IP és ETHERNET hálózatok a gyakorlatban 2. fej.

[32] Andrew S. Tannenbaum, Prentince Hall – PANEM 1999 Computer Networks. Third edition. 661. oldal 7.2. DNS – Körzeti névkezelő rendszer

[33] No, ennek az útnak a leírása több adatbiztonsági kérdést is felvet: 1. Az elküldött információ tartalom, sérüléstől mentesen továbbítódjon. 2. Az elküldött információt a címzett és csak a címzett kapja meg. 3. Az úton lévő információt csak a címzett tudja elolvasni.(titkosítás)

matematikusok úgy látszik zömmel szótlan férfiak, és keveset trécselnek, ezért eggyel, úgy tűnik nem számoltak.
Miként tudom elküldeni a levelet, ha közben a szóba jöhető továbbítók, mindenki a szomszédjaival trécsel, hogy ki kit ismer és honnan, közben pedig nem a levelet továbbítja?

Trécselés. Ha trécselésre kényszerítenek, vagy ilyen tartalommal túlterhelnek egy hálózatot, akkor az előbb lelassul majd, végső soron megbénul. Megáll az adatforgalom. Ez pedig így már, egy alapvetően informatika biztonsági kérdés. Az informatikai rendszereket trécselésre lehet bírni, és így be lehet dugítani.
Ez a problémakör már a Kritikus Infrastruktúra védelméhez is és a **büntetőjog témaköréhez**[34] is kapcsolódik.

A **hálózatok összeomlásának egy másik** (szintén matematikusok által is vizsgált) esete, amikor a hálózati gráfban az adatforgalom szempontjából keletkezett un. **természetes csomópontok** alakultak ki. Ezek olyan véletlenszerűen kialakult csomópontok, melyek a hálózatok fejlődésének természetes velejárójaként jöttek létre, és rajtuk bonyolódik a hálózat adatforgalmának jelentős része.

Az ilyen csomópontokat olyan adatmennyiséggel lehet elárasztani, amelyet azok nem képesek kezelni és ez által, mint csomópont megbénulnak. Ez a problémakör is a Kritikus Infrastruktúra védelméhez is és a **büntetőjog témaköréhez** [33] is kapcsolódik.

Ilyen csomópontokat láthatunk az ábrákon többek között az 1-es, 3-as csomópontokban. Ezek a hálózat fejlődésével kiemelt szerepet kaptak és több más csomóponttal tartanak kapcsolatot.

Az ilyen kommunikációs csomópontok sérülése kezdetben nem okoz nagy problémát egy redundáns hálózatban. A konkuráló adat továbbítási útvonalak ugyanis mintegy kiváltják a megsemmisült (kiesett) csomópontot.

[34] [33] Forrás: A Szerzőnek a Legfőbb Ügyészség egyik pályázatán, a Legfőbb Ügyész különdíját nyert pályaműve 25.-30. oldalig.

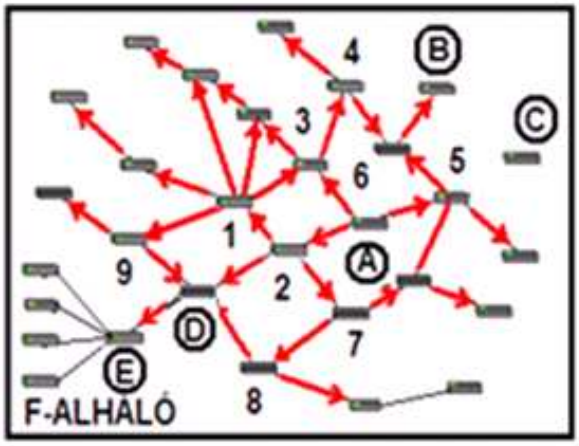
Ha az ábrákon látható módon A-ból B-be akarunk adatot küldeni, akkor azt három féle (különböző átviteli sebességű) rendszeren tudjuk megtenni. Az ábrákon ezeket vizsgáltam.
Az A-B küldés legsebezhetőbb pontja a 6-os csomópont. Ennél lényegesen kedvezőbb helyzetben van egy esetlegesen A-D pontba küldendő adat, amelynek számos egyenrangú útvonala is van.
Az A-ból C-be küldés pedig nem lehetséges, mert C nem része a hálózatnak. (Nem eleme a halmaznak)

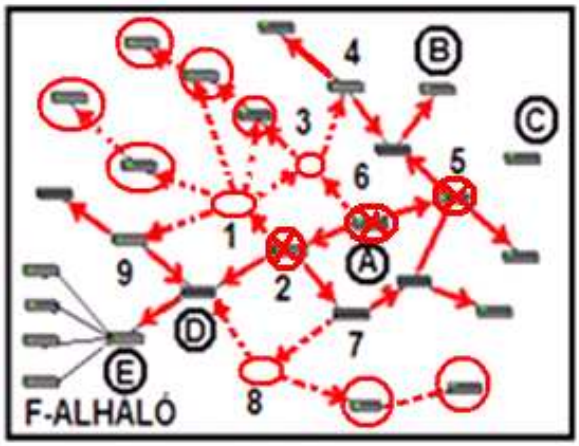
Végül: E és F-ALHÁLÓZATA pontok között – pl. egy cégen belüli hálózatban – akkor is fennmaradhat az adatforgalom, ha 8-as csomópont kiesik, tehát a rendszer összeomlás a 8-as csomópontnál megáll, vagy legalábbis tovább nem eszkalálódik.(Helyi szinten ezt úgy érzékeljük, hogy nincs internet és távoli adatelérés, de van LAN.)

ÖSSZEOMLÁS ELMÉLETEK:

BROADCAST összeomlása:

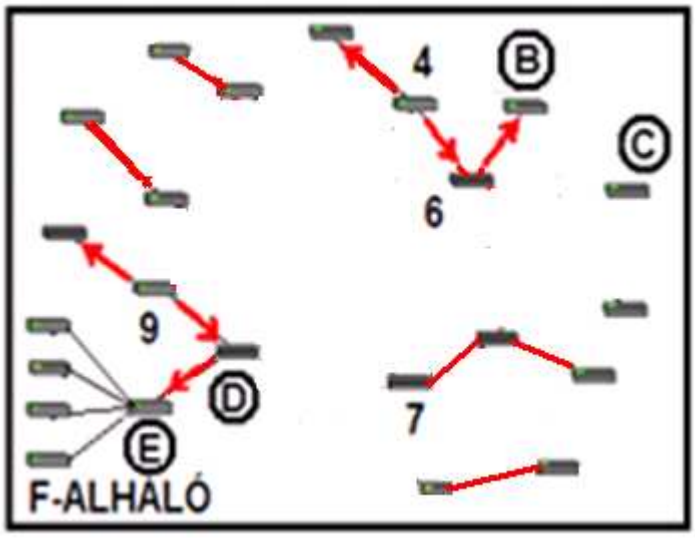
Az alábbi ábráim alapján könnyen belátható, broadcast esetén a hálózati útvonal hiánya nem lesz probléma pl az 1-es csomópont kiesésével, és még a 3-as és 8-as kiesése sem okoz útvonal problémát. Okoz viszont hálózati trécselést, mert a kiesett HUB-ok helyett túlgerjed a broadcast keresési forgalom, ezekkel a rendszer bedugul és ezért áll le. Ezt más megközelítésben a forgalom Dominó-elv szerű összeomlásának tekintjük.





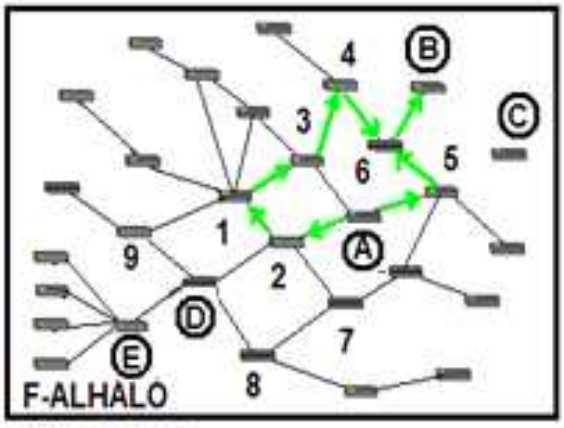
Az második ábrán látható helyzetben, a valamilyen külső behatás miatt kiesett HUB-okat üres piros karikával ○ és a kiesett továbbítási irányokat szaggatott piros vonallal - - - jelöltem. A másodlagosan az átterhelődő adatforgalom miatt megbénuló további csomópontokat kereszttel áthúzott piros karika ⊗ mutatja.

Az alábbi ábra **az „igazság pillanata”** az összeomlott rendszer maradványai, amin még van adatforgalom. Látható, lehetséges elszigetelt adatforgalom a perifériákon és lehet működés elszigetelt alhálózatokon is ilyen pl.: F-ALHÁLÓ.

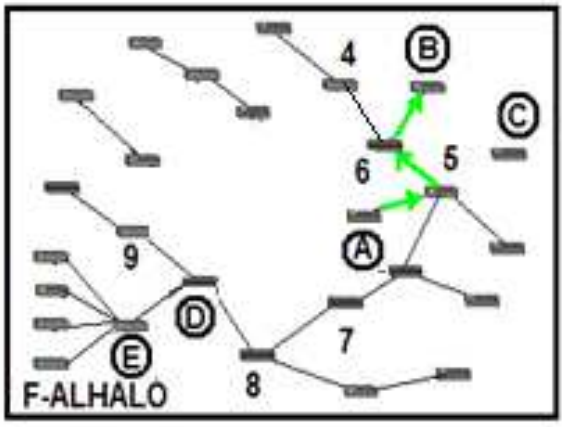


MULTICAST összeomlása:

Látható A-ból B-be történő adatforgalom szempontjából, multicast esetén, az 2-1-3-4-6 útvonalon 2,1,3 csomópontok kiesése nem kritikus, mert alternatívan 5-6 útvonal rendelkezésre áll. A kritikus csomópont ebből az útvonalból a 6-os. Multicast esetben nem beszélhetünk Dominó-elvről, mivel itt az adatforgalom behatárolt, meghatározott útvonalak kiesése, nem jár dominó effektussal, mivel a hálózati rétegben meghatározott számú útvonal vesz részt.



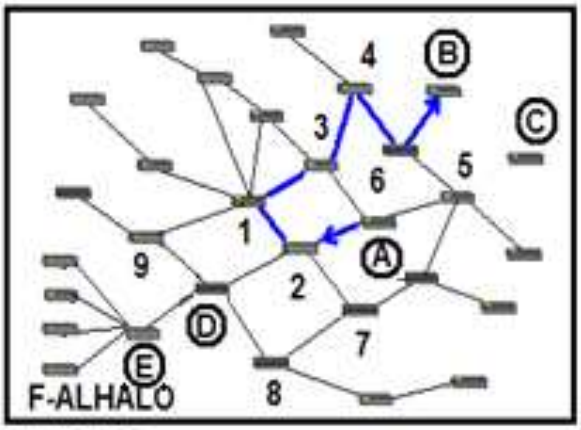
MULTICAST



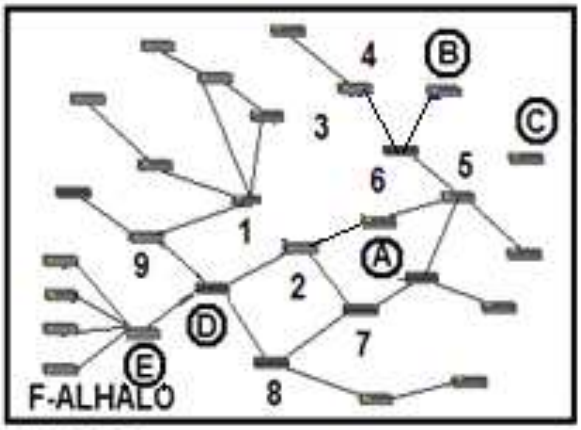
MULTICAST

UNICAST összeomlása:

Bármely elem kiesése a 2-1-3-4-6 útvonalon egyenrangú, A-ból B-be a kapcsolat megszakadáshoz vezet. Unicast esetben gyakorlatilag Point-to-Point kapcsolatot generálunk egy megadott path (útvonal) létrehozására, így ebben és ennek kihatásaiban nem szerepelhet kiterjedő, eszkalálódó hatás. Persze az útvonalon kieső nagy csomópontoknak lehet eszkalálódó hatása.

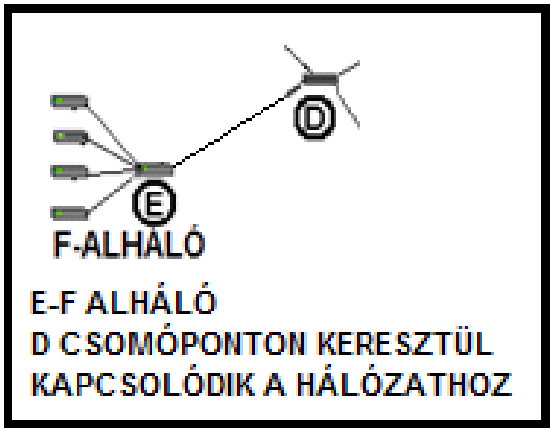


UNICAST

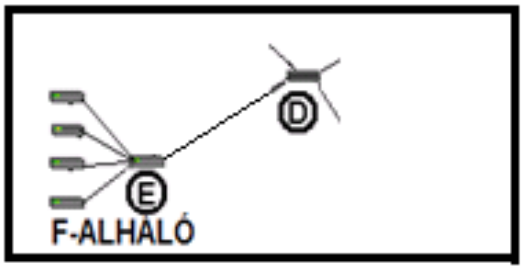


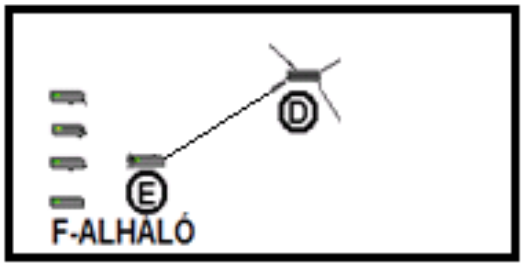
UNICAST

E-F ALHÁLÓ összeomlása:

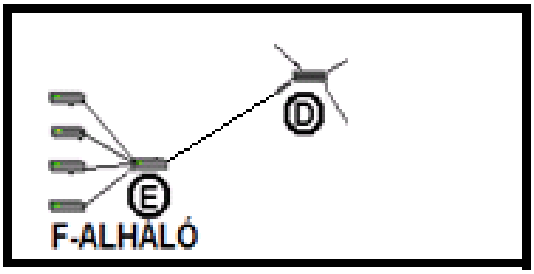


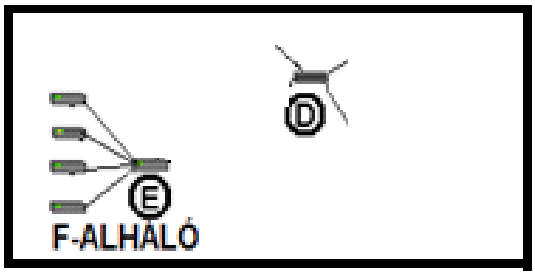
F-ALHÁLÓN belüli kiesés, nem hat ki a külső hálózatra. Nem eszkalálódó esemény.





Az E-F ALHÁLÓ **belső forgalmában** a Hálózat kiesése nem vált ki hatást. A kifelé való kommunikáció azonban ez által megszűnik.





Amennyiben olyan nagyszámú csomópont esik ki, hogy az unicast és multicast útvonalak fenntarthatatlanná válnak és az adatforgalom a megmaradt broadcastra hárul, úgy ez utóbbiakban bekövetkezhet a dominóhatás. A rendszer e ponttól fenntarthatatlanná válik és az adatforgalom (hasonlóan az első esethez bedugul) végül megszűnik.

Rendkívül sérülékeny a B cím szempontjából a 6-os csomópont. Különösebb matematikai levezetés nélkül belátható, kiesése esetén B-ben nem továbbítható adat. Tehát ezt érintő hálózati hiba az adat forgalom megszűnésével érinti B-t. C pontba semmilyen körülmények között nem küldhető adat mivel ez kívül esik a hálózaton (nem eleme a halmaznak) F-ALHÁLÓZAT köszöni szépen, jól elvan magában.

A probléma megoldását e sorokat olvasva még nem tudjuk, de már vannak kérdéseink, amiket azért majd igyekszem később megválaszolni.

A fő kérdés mi okozza a túlterhelést, és miként lehet az megszüntetni?

Meddig tart a hálózat túlterhelése?

Okozhat-e a túlterhelés károsodást a hardverben?

Megnyomhatom-e ezt a piros gombot, amire az van írva „RESET”?

Hol van? Melyiket?

Mi van, ha mindent gyorsan kikapcsolok?

Kikapcsolhatok mindent gyorsan?

Mi a gyors?

Írjuk fel ezeket a kérdéseket, mert később más szemszögből vizsgálva a témát, hasonló kérdésekre kell visszatérően választ kapnunk és lehet, hogy hasonló válaszaink lesznek.

Mennyit ér a micsoda, kinek és mikor?

Az informatikai rendszerek értéke, azaz amit meg akarunk menteni - kezdve az okostelefonon, laptopokon és háztartási PC-ken az internettel, folytatva a KKV-k által működtetett vállalkozási szervereken és LAN-WAN rendszereken át a nagyvállalati telekommunikációs, banki, börze és más szervertermeken keresztül a saját globális kapcsolatokkal rendelkező adat központokig… - a mai napig **nem tisztázott fogalom.**

Az érték viszonylagos gondolati fogalom, kinek, mikor mennyit ér valami. Szeretjük pénzben kifejezni, pedig az **érték előbb volt erkölcsi kategória**.

Kérdés az, hogy a társadalmunkat fenntartó informatikai rendszereknek tulajdonítunk-e erkölcsi (irracionális) érték kategóriát. Az tény a Tízparancsolat nem említi. De azért jogos kérdéseket lehet felvetni: erkölcsi érték-e az információ szabadság? Erkölcsi érték-e az adatállományok biztonsága? Vesztett-e erkölcsi értéket is az emberiség az alexandriai könyvtár 500.000 tekercse elpusztulásával?[35]

Ha egyik napról a másikra nem lenne informatika, mit vesztenénk?
Ez költségkérdés?

Hát nézzük, milyen érték megközelítési lehetőségek is vannak. Sajnos, mint azt az előszóban már jeleztem, a kidolgozással jelen dolgozat keretei között adós maradok, de azért gondolatmenetem szempontjából érdemes felvetéseimen elgondolkodni.

Az IT értéke adójogi, számviteli szempontból a bekerülési költséget, működési költséget és amortizációt veszi alapul, ahol az adott költséghely eszköz, üzemeltetés költségeinek és élőmunka ráfordításainak valamint a

[35] Az alexandriai könyvtár az ókori világ legnagyobb könyvtára volt. A Kr. e. 3. században hozták létre Egyiptomban, elsősorban a Museionban folyó kutatások elősegítésére és a görögök szellemi örökségének megőrzésére. A Könyvtár először Kr. e. 48–47-ben, az alexandriai háború idején égett le. A végső pusztulás Kr. u. 640–642 között következett be.

bevételeinek összességét, az amortizációval csökkentve mutatja. Ebből a szempontból megkülönböztetünk **könyvszerinti** és **üzleti** [36] értéket.

Más elemzők az **informatika cégérték szemlélet**ében [37] azt vizsgálják, milyen hozzáadott értéket képvisel illetve milyen cégérték változások következnek be az informatika fejlesztésével és a vállalati menedzsment IT irányú súlyponteltolódásaival. Ez nyomon követhető a cég részvény értékének változásaival ekként az IT (pénz) érték teremtővé léphet elő.
Prof. Dr. Martin Curley az Intel Labs Europe igazgatója számos előadásában ismertette az általa készített IT CMF fejlődési modellt, amely azt bizonyítja, hogy az IT fejlődése a korábbi költséghely szerepből és a nyújtott szolgáltatás definiálásán túl, mára proaktív gazdasági szerep lett, amely nem követi, hanem utat mutat a cégek gazdasági fejlődésének.

Az IT-CMF érettségi szintjei

Érettség		Az it mint üzleti vállalkozás	Az it-költségvetés kezelése	Az it-képességek kezelése	Az it értékteremtő képességének kezelése
Magas					
Optimalizált	5	Értékközpont	Fenntartható gazdasági modell	Vállalati alapkompetencia	Optimalizált érték
Fejlett	4	Beruházási központ	Kiterjesztett finanszírozási lehetőségek	Stratégiai üzleti partner	Opciók és portfólió-menedzsment
Köztes	3	Szolgáltatóközpont	Szisztematikus költségcsökkentés	Technológiai szakértő	Roi és üzleti számítások
Alap	2	Költséghely	Kiszámítható teljesítmény	Technológiai szállító	Teljes költség számítása
Kiindulás	1	Kezdetek			
Alacsony					

Egy másik megközelítési mód, az **IT szolgáltatási értékének** megközelítése felől, megnézzük azokat a károkat, amelyek a rendszer **kiesésével,** hiányával állnak elő és ezekből keletkezett **származékos**

[36] 2004 Budapesti Corvinus Egyetem, Gazdálkodástani Doktori Iskola, Juhász Péter PhD. értekezés, témavezető Dr. Reszegi László, egyetemi docens. Címe: „Az üzleti és könyv szerinti érték eltérésének magyarázata – Vállalatok mérlegen kívüli tételeinek értékelési problémái"
[37] Information Technology Capability Maturity Framework, 2009. kidolgozója Prof. Dr. Martin Curley. Forrás: http://www.itbusiness.hu/hetilap/cimlapon/Informatikabol_uzleti_ertek.html

károkból vezetjük vissza a tényleges értéket. Tehát a „káros eredmény” oldaláról közelítünk a problémához.
Az **IT értékének** egy még másik megközelítése, ha megnézzük **helyettesíthetjük**-e illetve milyen **helyreállítási költséggel** pótolhatjuk és egyáltalán pótolhatjuk-e az elveszett IT képességeket.

A keletkezett kár lehet hardverben, hálózati kapcsolatokban, működtető rendszer szoftverben vagy alkalmazásban és létrejöhet, az adatállományokban valamint keletkezhet áttételesen származékos kárként. A származékos kárt tekintjük lényegesen nagyobb veszélynek.(Ha nem hiszi, kérem, lapozzon a 28. oldalra és olvassa el a példát.)
Még akkor is belátható, ha ebben a megközelítésben a károkat a pótlási, vagy helyreállítási költségekkel (reparáció) alapul véve közelítünk az értékhez.

Adjunk nevet ezeknek a módszereknek:
- Pénzügy-számviteli értékelés
  - könyvszerinti érték
  - üzleti érték
- Cégérték alapú értékelés
- Származtatott kár alapú értékelés
- Helyettesítési és helyreállítás alapú értékelés

Mindegyik érték meghatározás pontatlan, ugyanis az értéknek **időfaktora** [38] van. Ami ma érték, nem biztos, hogy holnapra is érték marad. Az érték, mint az értékrend megtestesülése időben devalválódhat különösen, ha az érték pusztulásával az értékrend is válságba kerül, azaz megkérdőjelezi saját korábbi értékeit…

Ki akar egy a pusztulással, vagy károsodással vitatott értéket helyreállítani és ennek érdekében képességeit maximális készséggel latba vetve dolgozni

[38] Forrás: Miskolci Egyetem, Vállalkozáselmélet- és Gyakorlat, Doktori Iskola
Várkonyiné Juhász Mária 2008 PhD. értekezés.
Doktori Iskola vezetője: Dr. Nagy Aladár egyetemi tanár, a közgazdaságtudományok doktora. Témavezető: Dr. Pál Tibor egyetemi docens, a közgazdaságtudományok kandidátusa,
Címe: „Az érék fogalmának változásai és könyvvizsgálatának kérdései a hazai szabályozás tükrében.”
Hivatkozott szöveg a 31. oldalon: „Az organikus mérlegelmélet célja egymás mellett és azonos súllyal szerepeltetni mind a reális vagyonérték meghatározását, mind a reális eredmény kiszámítását. A vagyon reálértékének meghatározása **időérték elv** alkalmazásával történik napi árakon értékelve…”

az érték újra teremtésén? Márpedig a dolgok károsodása, vagy pusztulása mindig felteteti velünk ezt a kérdést, **mit ér meg az értékünk védelme?**
Azaz a pusztulással, károsodással egy döntési helyzet áll elő.
Dönteni kell, és gyorsan kell dönteni.

Gyorsan kell dönteni, mert hatékonyabbnak és gyorsabbnak kell lennie a védekezésnek, helyreállításnak, mint az okozott kár eszkalációja előrehaladásának. E versenyfutás megnyerése a rendszer sokk elkerülésének egyetlen járható útja.

Ugyanakkor a gyorsaság-költség függvény exponenciális jelleggel látszik növekedni, és a készségszintű képességet csak tréninggel és sok-sok gyakorlással lehet megfelelő szinten tartani és ez is költség.

ÉS MEGINT az időfaktor. Minél gyorsabb a beavatkozás, annál kisebb az okozható kár. DE ERRE TRÉNINGEZNI KELL!

Hesz Mihály [39] olimpiai bajnok kajakozó öltözői szekrényében volt egy, az ajtóra belülről felírt mondat, amelynek az értelmét, az 1968-as mexikói olimpia K-1 1000 méteres döntőjében be is mutatta a világnak. A cél előtt 100 méterrel még az 5.-6. helyen kajakozott, több mint egy hajóhosszal lemaradva az élen levőktől. Már-már mindenki lemondott még a dobogós helyezés reményéről is, 7-8 méter hátrányt lefaragni lehetetlen, de ekkor józanésszel felfoghatatlan véghajrába kezdett. Az utolsó métereken nemhogy behozta ellenfeleit, hanem olimpiai arany érmet szerezve az első helyen érkezett a célba.

Az a mondat a szekrényében ez volt:

„A gyorsaság nem kirobbanás, hanem kompozíció”

Hesz Mihály több mint tizenöt évig edzett és edzett és készült erre a győzelemre.

Tizenöt év edzés, gyakorlás és 30 másodperc a bizonyításra ez az arány…

[39] Forrás: Magyar Sportenciklopédia A-K Kossuth kiadó 2002. 397- 415 oldalak,
Hesz Mihály Született: 1943. december 15., Nógrád, Egyesületei: Váci Hajó, FTC Legjobb eredményei: olimpiai bajnok (K-1 1000 m, 1968); olimpiai 2. (K-1 1000 m, 1964); 2x világbajnok, sokszoros Eb helyezett.

Döntési modellek.

Az informatikával foglalkozóknak is napi tréningben kell lenniük, ha jön a „futamuk” nyerni tudjanak, ez költséges elismerem. Hogy mikor kell indulni és merre az pedig vezetői döntés kérdése. Veszélyhelyzetben gyorsan (automatikusan) kell dönteni, már előre kidolgozott minták alapján, bízva a rendszerben.

A döntések tudományos szintű vizsgálatával az operációkutatás és döntéselmélet-módszertan tudománya foglalkozik.
Az operációkutatás[40] és döntéselmélet abból indul ki, hogy ha a döntéselméleti térben, leírhatóak (vannak) olyan érték – költség – idő függvényeink, amelyek valahogy viszonyulnak (viszonyíthatók) egy-vagy több célfüggvényhez, akkor ezek vizsgálatával előre kiválaszthatóak (prognosztizálhatók) azok a döntési alternatívák, amelyek adott döntési helyzetben optimálisak, vagy ahhoz közeliek és elemzésükkel feltárhatók a folyamatok rejtett hatásai is.
Ezek a függvények lehetnek ténylegesen leírt matematikai (ábrázolható) függvények és lehetnek adat idősor mátrixok, vagy halmazok. A függvénygörbék lefutása alapján beszélhetünk lineáris programozásról illetve nem lineáris programozásról.
A paraméter és a célfüggvények összevetéséből lehetséges az optimális döntés meghozása. Ezekben a döntésekben tehát előre „behuzalozott” értékeknek kell lennie, amely már előre számol a veszteségekkel, nyereségekkel és nem esélyeket latolgat, hanem döntési alternatívákat ad.

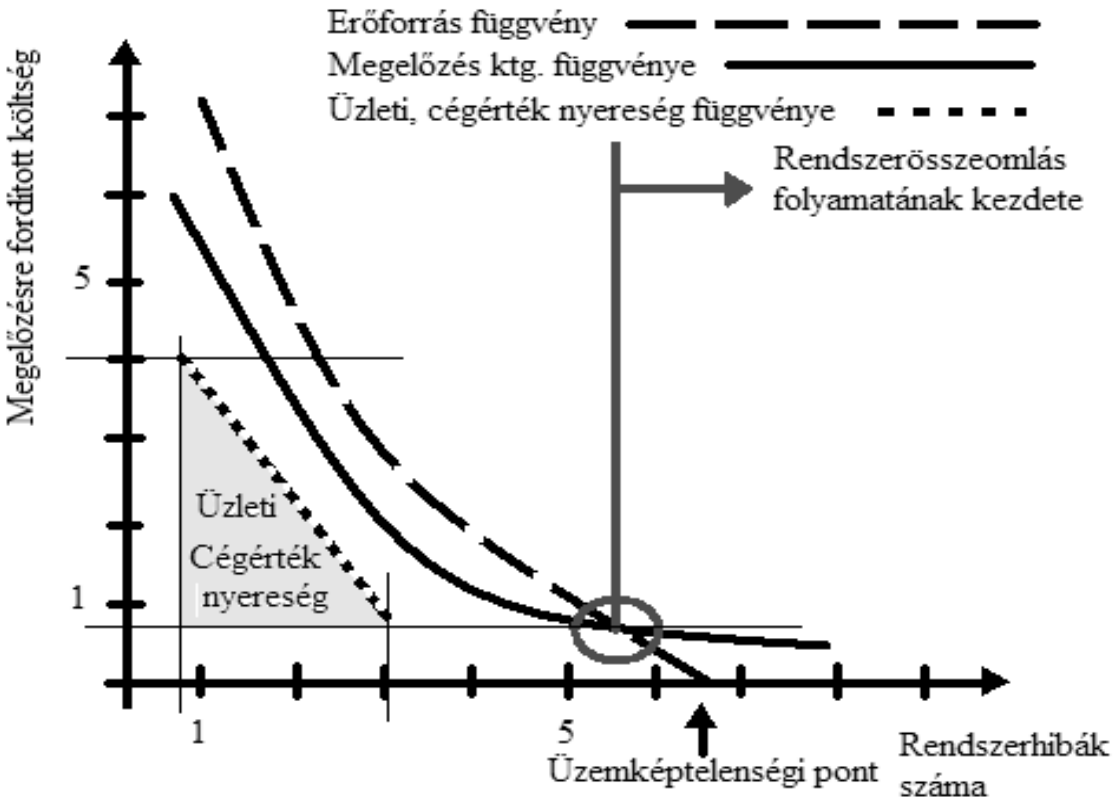
Érdekes elméleti modellt alkottam és ezzel egy döntési kísérletet végeztem egy elképzelt vállalti rendszer fatális tönkremenetele kapcsán.

[40] Glevitzky Béla, Operáció kutatás 1. mobiDIÁK könyvtár sorozat, Kiadó: Debreceni Egyetem 2003.

Az üzleti gazdaságossági optimumra beállított, megelőzési költség modell.

Azt vizsgáltam, milyen következtetéseket lehet levonni egy olyan grafikus döntési modellből, amely három függvény közös optimumát kezeli.
Az egyik függvény, ha egy rendszer fenntartására forrás áll rendelkezésre és meghatározható egy (pénz) **erőforrás függvény**, amely a rendszerhibák száma és az erőforrás rendelkezésre állás közötti kapcsolatot írja le.
Továbbá, ha meghatározható egy **megelőzési költség függvény**, amely a hibák megelőzésére fordítandó összeg és a rendszerhibák száma közötti kapcsolatot írja le.
Valamint, ha meghatározható egy **üzleti, cégérték nyereségfüggvény**, amely egy vállalkozás üzleti és cégértékének (a nyereség) változása és a rendszerhibák közötti kapcsolatot írja le, akkor:

Milyen értéktartományban és milyen hiba sávban célszerű, gazdasági racionalitás alapon egy rendszert üzemben tartani?



Meglepő következtetéseket lehet levonni az ábrából, de először ismertetném a három függvény jellegét.

A „**megelőzési költség függvény**” azt jelenti, minél kevesebb hibát tűrünk meg a rendszerben, úgy az erre a megelőzésre fordítandó költség logaritmikusan emelkedik, és viszont eszerint is csökken. Minél több hibát engedélyezünk egy rendszer működésében annál kevesebb a ráfordítandó hiba megelőzési költség. Elvileg a hiba megelőzésre fordítandó költség lehet végtelen és elvileg, nem érheti el a 0-t csak tart hozzá, mert a rendszer létrejött és átadásra került. Tehát a megelőzésre fordított költség már bármilyen kicsi mértékben is, de a bekerülésben már benne van.
Azt hiszem ez így érthető.

Az „**erőforrás függvény**” azt jelenti, mekkora költség ráfordítási „keretünk” van a rendszer fenntartására. Belátható, magas erőforrás rendelkezésre állás mellett alacsony lehet a rendszerhibák mennyisége, és ahogy egyre kevesebb a fenntartásra fordítható erőforrás, úgy növekszik a hibák száma. Ez a függvény azonban biztosan eléri a nullát, mert a rendelkezésre álló erőforrás biztosan lehet nulla. Itt erőforrás tekintetében nem csak a vállalat saját erőforrásait kell érteni, hanem beszélhetünk más, bevonható külső forrásokról is.

Ebből az következik, hogy lefutástól függetlenül a fenti két függvényünk biztosan metszi egymást, tehát létezik fedezeti pont.

Az „**üzleti nyereség és cégérték függvény**” az a gazdasági limit, amíg egyszerűen a rendszert nyereségesen üzemeltetni lehet. Nyilván ha egy cég IT jól, kevés hibával működik, úgy a cég is folyamatosan dolgozhat és jó üzleti és cégérték (tőzsdei ár) értékeket[41] érhet el. Ez természetesen csak egy itt alkalmazott elvi korreláció. Ha több a hiba, úgy romlanak a gazdasági eredmények is. Tehát ez jó közelítéssel egy fordított arányos lineáris függvény lehet, amely bizonyosan a költség és erőforrás függvények alatt helyezkedik el. A költség függvény alatti elhelyezkedést nem kell magyarázni. Nem nagyon ismerek olyan legális vállalkozást, ahol a nyereség meghaladná a költségek szintjét. Az erőforrás függvény alatti elhelyezkedést pedig a külső források magasabb bevonhatósága indokolja.

[41] Information Technology Capability Maturity Framework, 2009. kidolgozója Prof. Dr. Martin Curley

Mi mindent olvashatunk le a döntési feladat grafikus megoldásából?

1. Az erőforrás függvény és hibák megelőzésére fordítandó költségfüggvény metszéspontjánál alacsonyabb erőforrás rendelkezésre állás esetén elkezdődik a rendszer összeomlásának folyamata. Ez gyakorlati üzemeltetői szempontból a **hiány**[42] állapotának felel meg. Az üzemeltetők folyamatosan „tüzet oltanak" az éppen jelentkező legfrissebb hibák folytonos elhárítása zajlik.

2. Az üzemképtelenségi pont az, amikor az erőforrás függvény eléri a nulla ráfordítást. E pont felett a rendszer fenntarthatatlanná válik.

3. Az üzleti nyereség és a cégérték által determinált helyzet, pedig ha sarokpontjait kivetítjük a vízszintes és függőleges tengelyekre, úgy az kijelöli a gazdaságilag értelmezhető rendszer megtartási zónákat. Ez rajzunkon azt jeleni, hogy 0,8 és 4 közötti megelőzésre fordítandó költség és 0,8 és 3 közötti hibaszám, ami mellett a rendszer nyereségesen üzemeltethető. Ezen összegek feletti ráfordítás már nem térül meg, jóllehet láthatóan lenne még rá erőforrás. Az ezen összeg alatti ráfordítás pedig már a rendszer összeomlásához vezető folyamat kezdete. (Fedezeti pont alatt van.)

4. Nincs egy optimális döntés, hanem a három függvénynek együttesen megfelelő optimum halmaz van. Ennek folyománya, hogy van lehetőség további célfüggvények figyelembevételére.

[42] Kornai János: A hiány. Közgazdasági és Jogi Kiadó 1980,1982,1989.

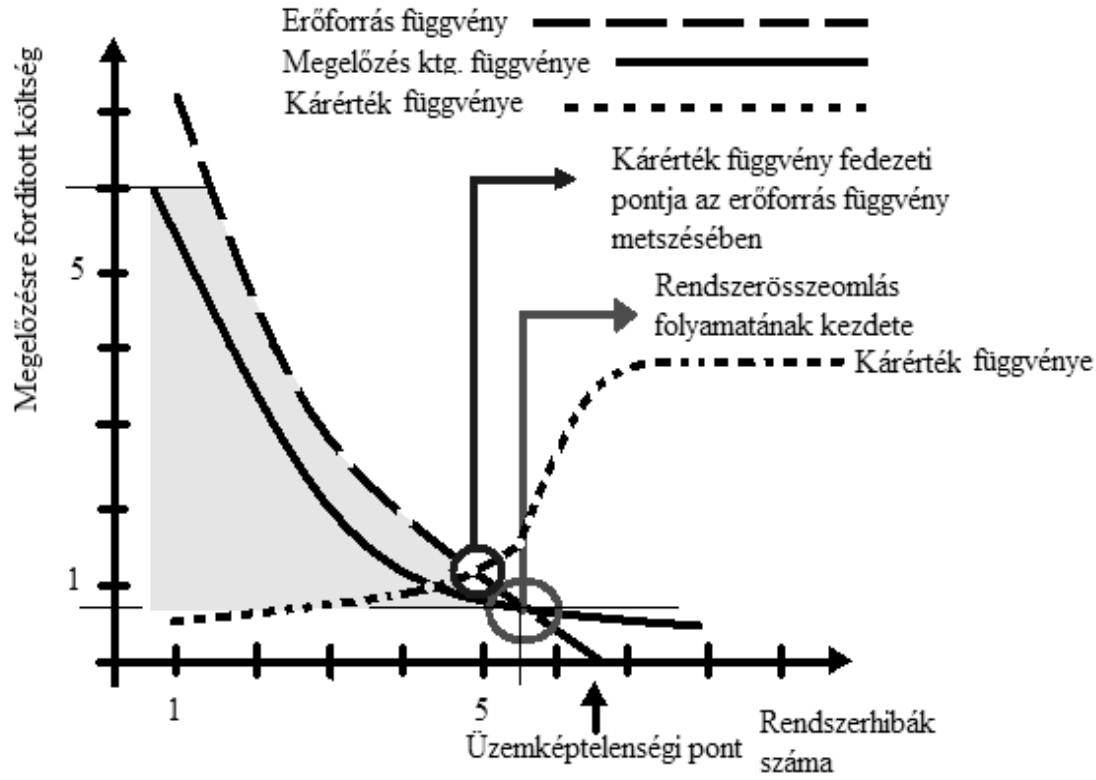
Az okozható kárérték optimumra beállított költség modell.

Itt megint vissza kell kanyarodnom, hogy az IT értéke lehet-e irracionális érték kategória? Amennyiben lehet, akkor az üzleti, cégérték függvény helyett más célfüggvényünknek – az okozható károkból kiinduló valószínűsíthető kárigénynek – nevezzük, **kárérték függvény**nek is kereshetjük az optimumát.

Ennek leírása hasonló az előzőekhez. Az biztos, hogy a hibák számának növekedésével növekszik a valószínűsíthető kárérték, és az is biztos, hogy elvileg nem lehet nulla, mert nulla hiba nincs egy valós rendszerben.

Azt is beláthatjuk, hogy a hibák szaporodásával nem egyenes arányban, hanem valószínűleg egy ponttól egynél kisebb exponenciális (gyökös függvény) szerint növekszik az okozható kárérték és ennek van egy maximuma, ami fölé nem mehet. (Ha minden kár megtörtént, ami megtörténhet, a kárfüggvény már tovább nem emelkedhet.)

A fent vázolt függvény modell az alábbi lehet:



A grafikus megoldást értelmezve, látható:

1. a gazdaságilag értelmezhető beavatkozási (lehetőség) terület a korábbihoz képest lényegesen nagyobb lett. Tehát ilyen helyzetben az erőforrás korlátja lép az üzleti, cégérték nyereségesség korlát helyébe.
2. Nincs egy optimális döntés, hanem a három függvénynek együttesen megfelelő optimum halmaz van. Ennek folyománya, hogy van lehetőség további célfüggvények figyelembevételére.

3. Irracionális érték kategóriákra annyit lehet költeni amennyink, van. Ez egyben a büdzsé szemléletet is jelenti. Nyilván itt már nem az üzleti korlát, hanem az erőforrás korlát érvényesül. Az erőforrás korlátossága szerint megkülönböztetünk **kemény és puha korlátot**[43], tehát amennyiben ezek közül az un. puha korlát érvényesül, amely rendszerint jellemzi az irracionális költségeket, akkor a mozgástér még tovább bővülhet, de ez már hatalmi / politikai alku kérdése.

4. Kiegészül azzal a látható ponttal, hogy a kárérték függvény és az erőforrás függvény fedezeti pontját meghaladó hibaszám felett már nem érdemes még ebben a szemléletben sem többet költeni, mert a várható kárérték, meghaladja az erőforrások lehetőségét.

Gondoljunk csak bele, ha egy interkontinentális pénzpiaci brókercég köt szerverbérlésre megállapodást, és kiesik a szerződött értéken felül a börzeideje – mekkora is lehet a kára? (Nézzük csak meg az előző oldalon a kárérték függvény maximumát mondjuk 1.000.000 kisbefektető néhány milliárd dollárjának árfolyamveszteségét egy szolgáltatás hiba miatt kimaradt tranzakció kapcsán…)

Talán még a teljes magyar államadóságot is ki lehetne fizetni belőle…

[43] Kornai János: A hiány. Közgazdasági és Jogi Kiadó 1980,1982,1989.

Költségtakarékos megelőző intézkedések

Ám ha minden költséges, akkor joggal vetődik fel a kérdés, „ha tudjuk, hogy el fogunk esni, miért nem ülünk le”, de legalábbis előre egy (több) **párnát kötözhetnénk a legfájóbb testrészünkre**…

Van ilyen **párnázó törekvés**, és mindjárt ismertetem is, de ennek megértéséhez előbb egy kicsit térjünk ki a beruházások szervezése és megvalósítása területére.

Erre azért van szükség, hogy tisztán lássuk, mikor kell a „párnázást” elkezdeni.

Elvileg és általában egy beruházás és itt az IT-t is értem, a szerevezés elmélet és módszertan szerint a beruházói igények összefoglalásával kezdődik.

Ez a módszertan, ám a valóságban hány és hány komoly beruházást láttunk, hallottunk életünkben, amely nem így zajlott vagy éppen nem így zajlik.

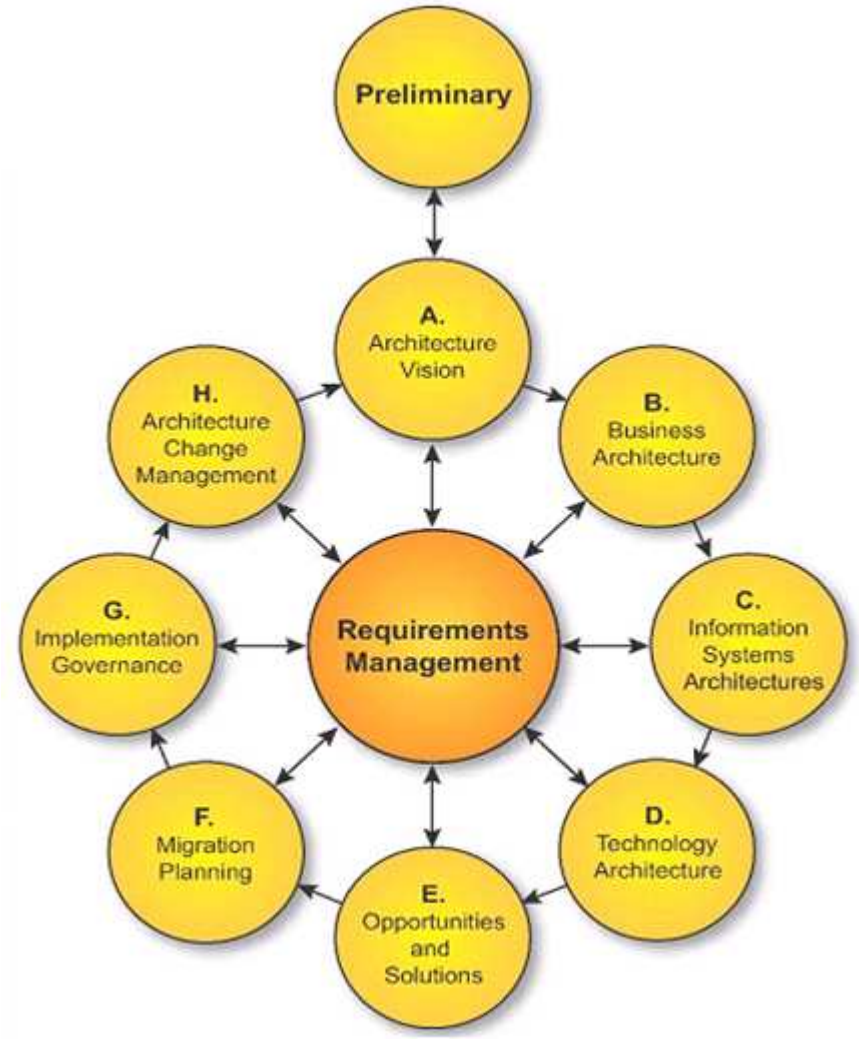
Hányszor írják felül a parciális helyi, vagy éppen tervezői presztízs érdekek a beruházás céljának alapvető meghatározását a beruházói igények összefoglalását…

Mert ez a kulcs, a beruházói igények összefoglalása.

Életem során volt szerencsém már jó pár ilyent készíteni, majd jobb sorsom okán megvalósítani. Szóval én ettem meg, amit magam főztem.

A beruházói igények összefoglalását a PRINCE 2 [44] módszertan a beruházás „prestart” fázisához köti.

A TOGAF [45] módszertan szerint az alábbi ábrán a „preliminary” (előkészítés) során, az A–H körben kerül meghatározásra.



Tehát, rendszerszemléletben az előkészítési fázist követi a tervezési fázis.

Ennek az értelme, hogy a kész beruházást nem a terveknek való megfelelés, hanem a beruházói igényeknek megfelelés minősíti. Ennek csak eszköze az alapos tervezés és körültekintő kivitelezés.

[44] PRINCE 2 módszertan: Forrás: http://www.prince2.com/prince2-structure.asp
[45] Ábra Forrás: TOGAF The Open Group Architecture Framework 2009. kiadás 88. oldal

Tehát a „párnázást” már a beruházás előkészítő fázisában meg kell kezdeni. Már ekkor tisztázni kell milyen és mekkora kockázatokra kívánunk tervezési programot készíttetni.

Hiába felel meg a szép, kész ház a kiváló és jó minőségű terveknek, ha a megrendelő egy bombabiztos vár építését akarta volna.

A beruházói igény összefoglalás alapján határozzuk meg, az un. tervezési programot. Ez azt írja le, hogy az építendő épületnek és/vagy IT rendszernek milyen követelményeknek kell majd eleget tennie és azt milyen mérnöki megoldásokkal kívánjuk elérni. Tehát a mérnökök erre a meghatározott célra terveznek. Persze bizonyos hiba határral. A Titanic óceánjáró tervezési célja az volt, hogy a világ legnagyobb és leggyorsabb hajóját építsék meg. Természetesen a biztonság is szerepelt a tervezési célok között, de Moldova György történetével illusztrálva „Erre azért nem gondoltam”.

A beruházói igény összefoglalás határozza meg, hogy a beruházó milyen nagyságú és milyen biztonságú rendszert akar. Ennek egzakt megfogalmazása azonban nehéz feladat.

Ezért a továbbiakban az ezt segítő eszközöket (szabványok, ill. ajánlások) fogom bemutatni.

Hogy kerül az ISO az asztalra?

Az **ISO**[46] rövidítés (Nemzetközi Szabványügyi Szervezet) jelenti, melynek speciálisan az informatikai rendszerek adat és működési biztonságára kialakított minőségbiztosítási, minőségirányítási rendszere az **ISO 27000**[35].

Ez tulajdonképpen az **ISMS**[47]. **I**nformation **S**ecurity **M**anagement **S**ystem. Információ Biztonsági Rendszer.

Örömmel dőlnénk hátra. Hurrá! Semmi más dolgunk nincs, mint kinyitni a szabványt és tenni, ami ott le van írva az IT működésére, tervezésére illetve működésének kiesésére.

Sajnos ez nem ilyen egyszerű.
Ez a szabvány (és általában a minőségbiztosítási szabványok is) csak azt írják le, hogy kinek milyen eljárásokat, milyen rendben kell A SAJÁT SZERVEZET SZÁMÁRA kidolgozni. Azokat mindenki a maga szervezetében miként tartsa be és miként gyakorolja, hogy az magas szinten elsajátított képesség legyen és ezeket a képességeket hogyan tartsa készség szinten meg.

„A gyorsaság nem kirobbanás, hanem kompozíció”

Az egyik ilyen kompozíció az ISMS.
Nem kész szer, amit használunk, hanem út, amin járhatunk.

Az edzés elmélet és módszertan a **sportmozgások adaptációjának** [48] több szintjét írja le. Az első adaptációs szint a **durva koordináció** szakasza, az adott sportmozgás leutánzása, annak tartalmi elemei nélkül. A következő

[46] Forrás: Magyar Szabványügyi Testület honlapja: „A Nemzetközi Szabványügyi Szervezet (International Organization for Standardization), rövid nevén az ISO, a második világháborút követően, 1947. február 23-án kezdte meg tevékenységét. Létrehozását "az ipari szabványok nemzetközi koordinálása és egységesítésének elősegítése" céljából 25 ország nemzeti szabványosítással foglalkozó képviselői határozták létre Londonban. A szervezet rövid neve, az ISO, minden nyelven ugyanaz, mert az nem a teljes név valamely nyelvű változatának kezdőbetűiből állt össze, hanem a görög *isos* szóból származtatták, amelynek jelentése *egyenlő*.”

[47] ISMS – Information Security Management Systems – Az ISO 27000 szabvány által leírt, speciálisan az informatikai rendszerek adat és működési biztonságára kialakított minőségbiztosítási és minőségirányítási rendszer.

[48] Dr. Nádori László: Edzéselmélet és módszertan, Testnevelési Főiskola tankönyv 83. oldal

szint a **finom koordináció** kialakulása, statikus mozgás modell, amelyben már a mozgás lényegi elemei megvannak és mindig azonos (ideális) kontrollált körülmények között a sportoló végre is képes hajtani. A legmagasabb szinten, amit **dinamikus adaptációnak** hívunk, a sportoló finomkoordinációja olyan magas szintjére jut, hogy gyorsan változó vagy akár kifejezetten gátló körülmények között is képes eredményes és sikeres tevékenységre.

Nos, az ISMS tulajdonképpen egy edzéselméleti „framework" amely **lehetőséget adhat** (SIC!) olyan **dinamikus belső vállalati szervezeti modell** kialakítására, amely nem csak adminisztratív korlátokat, hanem belső a Kritikus Infrastruktúrákat kezelő, üzemeltető személyzetnek megfelelő szintű MINDENNAPI TRÉNING LEHETŐSÉGET **biztosíthat** a kezelésükben lévő IT infrastruktúra hibáinak elhárítására dinamikus adaptációs szinten lévő képességek kialakítására.

Erre a már korábban említett **időfaktor miatt** van szükség.

Ha bizonyos tudomásom van róla, hogy képes vagyok (mert százszor gyakoroltam sikerrel) valamely hiba elhárítására (dinamikus adaptált képesség) akkor veszélyhelyzetben a készségem sem lesz gátolt saját felkészültségembe vetett bizonytalanságom miatt. Gyorsan és határozottan tudok cselekedni, képes leszek megnyerni a „futóversenyt" a gyorsan eszkalálódó problémákkal szemben.

Mit is írtam az előző oldalakon?

„A gyorsaság nem kirobbanás, hanem kompozíció"

Tizenöt év edzés, gyakorlás és 30 másodperc a bizonyításra ez az arány…

A készség szintű védelmi képességet fent kell tartani. Úgy gondolom, elvben mindenki bólogat, e sorokat olvasva. Egyetértünk. Nézzük az ISMS miként ad erre konkrét lehetőségeket, amelyeket már egy IT beruházás kezdetén figyelembe kell vennünk.

Már itt kezdődik a megelőző „párnázás".

Egyszerű javaslatok a beruházás előkészítő szakaszában az ISMS kialakítása kapcsán:

Az ISO 27001:2006 szabvány tartalmazza magukat a követelményeket melyhez a szabvány adaptációjában az általam javasolt, költséghatékony elemek lehetnek:

4.2.1 Az ISMS kialakítása.
b) 1)-5) pontban javaslom:
Célkitűzések között, a **vezetés kötelezze el magát** ISMS bevezetésére.
A Kritikus Infrastruktúrát kezelő személyzetet részesítsék **vészhelyzeti képzésben** és ennek tárgyi feltétele, a kockázatkezelési környezetbe a **képzést szolgáló elkülönült +1 infrastruktúrák** bevétele vagy ennek más módon történő biztosítását.

- Ezt át kell vezetni a beruházási igényterveken és a tervezési programon és a gazdasági terveken (lásd: erőforrás függvény)
- Vezetőség kötelezettséget vállal ezen, források biztosítására.
- Más módon történő biztosítás esetén, a kapcsolódó szerződésekkel kell biztosítani és át kell vezetni a gazdasági terveken.

4.2.2. Az ISMS bevezetése és működtetése
e) ponthoz: A képzési és tudatosítási programnak azokon a területeken ahol **manuális vagy IT kezelési képességek** is szükségesek, ott a képzésnek gyakorlati képesség szintjén el kell jutnia a beavatkozások végrehajtásának legalább a finom koordináció, de inkább a dinamikus adaptáció szintjére.
A **tudatosítási program**nak el kell jutnia az ISMS folyamatainak interiorizálódásához.

4.2.3. Az ISMS figyelemmel kísérése és átvizsgálása
a) 4) ponthoz: Biztonsági incidensek megelőzésének **proaktív gyakorlása** a képzést szolgáló +1 infrastruktúrákon.

4.2.4. Az ISMS fenntartása és fejlesztése
d) Az érintett személyzet felé visszajelzés a **jelzett** képzések eredményéről.

5.2. Gazdálkodás az erőforrásokkal
5.2.2. Képzés, tudatosság és felkészültség
a) - d) pontokhoz: Térjen ki ezen, folyamat **pedagógiai fejlesztő** jellegére.

6. Belső ISMS - auditok
d) Elvárás a **pedagógiai elfogadható**ság ellenőrzése is.

7. Az ISMS vezetőségi átvizsgálása
7.2. Az átvizsgálás bemenő adatai
b) ponthoz: Az érdekelt **személyzet véleményezze** a kapott képzések szakmai színvonalát, gyakorlati alkalmazhatóságát.

8. Az ISMS fejlesztése
8.2 Helyesbítő tevékenység
d) ponthoz: a szükséges helyesbítő tevékenység térjen ki a vészhelyzeti és egyéb célirányos képzések javítására.
8.3. Megelőző tevékenység
c) – d) pontokhoz: a szükséges **megelőző tevékenység és annak gazdasági tervezése**, figyelemmel a megelőzési költség függvény alakulására. Lásd: TIA942.

Elnézést kérek, már megint a költségeknél – költség függvényeknél – kötöttünk ki, és annál, hogy TIA 942.

Mi is az a TIA 942?
És hallják a trombitaszót? Miért? Trombitálnak?

TIA 942, hát ez meg mi a szösz?
A TIA 942, mint megelőző eszköz…

Én hallom a trombitaszót, talán más is. Mert trombitálni kell, folyamatosan. Addig trombitálunk, amíg van (másik) trombitánk. Hogy legyen másik a zsebünkben az a megelőzés, és hogy ez mibe kerül ez a megelőzési költség függvény.(Szomorú vagyok már megint a **kályhához jutottunk** [49]vissza.)

Talán vannak mások is, akik látták a cirkuszi bohóctréfát. A bohóc hangosan trombitálva jön be a porondra, de a porondmester elveszi tőle a hangszert, hogy ne trombitáljon, de az a bohócruhája zsebeiből mindig újabb és újabb trombitaszerű hangszereket húz elő „ Nem baj, van másik! ” felkiáltással boldogan trombitál tovább. (*Erre mondhatná egy TIER szakértő, hogy többszörösen redundáns a trombita rendszere*.)

Ilyen az informatika is. Trombitálunk. Folyamatosan. Szünet nélkül.
Mennyire szünet nélkül? Nagyon szünet nélkül. Nem viccelek, tényleg.

Annyira komoly a dolog, hogy nemzetközi szabvány **TIA 942**[50] rögzíti egyes biztonsági fokozathoz (TIER 1,2,3,4) tartozó informatikai rendszerek éves „trombitálási” üzemelési (rendelkezésre állási) idejét, és azt hogy ezt miként kell-lehet elérni és fenntartani. Ebben megdöbbentő számok vannak.

A szabvány részletes ismertetésére, jelen értekezés terjedelme miatt nem térek ki, de a fő gondolatai ismertetem:
Az adatközpontok (és a benne lévő alrendszerek) biztonságát 4 fokozatba sorolja, telekommunikációs infrastrukturális környezeti **tartalék** és **hibatűrés** fogalmakkal, a fokozatot **TIER**[51] – nek nevezünk.
A szabvány két nagy kérdéskört érint: egyrészt meghivatkozza azokat a konkrét anyag felhasználási és kivitelezési előírásokat tartalmazó más szabványokat, amelyeket alkalmazni kell és „framework” (keretajánlás)

[49] Lásd: Jelen tanulmány csak a leglényegesebb elemeiben érinti a szabványt és alkalmazási területeit.
[50] Telecommunications Industry Association – az USA és Kanada Telekommunikációs Ipartestületei által közösen az Amerikai Nemzeti Szabványügyi Intézettel (ANSI) összhangban kiadott szabvány az adatközpontok biztonsági szintjeinek meghatározásához és besorolására: un.: TIER 1-2-3-4 fokoztok.
[51] Telecommunications Infrastructure Environment Redundancy – TIER szójáték, telekommunikációs infrastrukturális környezeti tartalék mozaikszava, de üléssort is jelent angolul: ti. hányan férnek el.

formában kidolgozott elképzeléseket ad az adatközpontok kialakítása számára az alábbiak szerint.

A szabvány koncepciójában van **tartalék** és van **hibatűrés**, amit a szabványhoz fűzött **IVSZ** [52] ajánlás a magyar kivonatban így tárgyal:

Tartalék: További egység biztosítása a normál működéshez szükséges darabszám (**N**) felett. Jelölése: **N+1** Jelentése: Például, ha öt generátor szükséges az adatközpont tartalék energia ellátásához, akkor egy hatodik is biztosított. A gyakorlatban ezt a redundancia szint egy berendezéshiba tűrést és párhuzamos karbantarthatóságot biztosít.(*Még egy trombita*)

Egyszeres hibatűrés: Kétszer annyi egység biztosítása, mint amennyi szükséges. (egyszeres hibatűrés) Jelölése: **2N**.

Egyszeres hibatűrés plusz tartalékkal: Kétszer annyi egység, plusz még egy tartalék egység biztosítása, mint amennyi szükséges. Jelölése: **2N+1**

Kétszeres hibatűrésű rendszer: Két N+1 redundáns rendszer felépítése egymással párhuzamosan. (kétszeres hibatűrés) Jelölése: **2*(N+1)**

Az ajánlással érintett adatközponti méreteket a szabvány 3 csoportba [53] sorolja:

H1	Small Data Center	Server Room / szerverszoba
H2	Corporate Data Center	Server Center / szerverterem
H3	Large Data Center	Data Center / adatközpont

Biztonsági fokozatok vázlatos felépítése illetve egymásra épülése:

TIER 1 Nem redundáns fokozat, minden eszközből egy-egy van. Gyakorlatilag ez az N. (Értsd: 1xN)

TIER 2 TIER 1 + egyes a szabványban előírt rendszerekben előírt +1 tartalék van. Jelentése: N+1

TIER 3 TIER 2 + egyes a szabványban előírt rendszerekből előírt még egyszeres hibatűrés és egyes (nem duplikált) elemekben tartalékkal van ellátva. Jelentése: 2N+1

TIER 4 TIER 3 + egyes a szabványban előírt rendszerekből duplikált teljes rendszer van tartalékkal ellátva. Kétszeres hibatűrésű rendszer. Jelentése: 2*(N+1)

[52] IVSZ: Informatikai Vállalkozások Szövetsége ajánlása, 2010, Iparági egységes fogalomtár v11
[53] TIA 942 szabvány H melléklete (Annex H, H1. H2. H3.)

A TIER 1-4 biztonsági fokozatokkal érintett rendszerelemek:

- Építészeti kialakítás
- Elektromos ellátás
- Tűzvédelem
- Vízellátás és szűrés
- TELCO helyiségek kialakítása
- Data Center kábelezési rendszere
- Szerverhelyiségek hűtése

Visszatérve a trombitálásra, ezek a redundanciák mind arra szolgálnak, hogy az adatközpont folyamatosan és **lehetőleg megszakítás nélkül** tudjon dolgozni akkor is, ha közben az adatközpontban, vagy akár magukon a **működő szervereken menetközben hibajavításokat** eszközölnének.[54]

Egy évben menny időt képes egy rendszer folyamatos, megszakítás nélküli üzemben tölteni. Ezt nevezzük **rendelkezésre állásnak**. A TIER szerinti adatközpont rendelkezésre állás éves % és kiesési időre vonatkozó táblázatát az alábbiakban ismertetem:

Fokozat állás	Rendelkezésre (számított)	Éves állás idő
TIER 1:	99.671%	28 óra 49 perc
TIER 2:	99.741 %	22 óra 41 perc
TIER 3:	99.982 %	1 óra 35 perc
TIER 4:	99.995 %	26 perc

Ezek azért lényeges számok, mert egy meghatározott fokozatú adatközpontban elhelyezett szerver bérlése esetén az **ITIL**[55] szerint kötött **SLA**[56] (szolgáltatási szint) megállapodás ezeket a rendelkezésre állási

[54] Ajánlom a kedves Olvasó figyelmébe jelen tanulmány 61. oldalán a 2. képen ismertetett megoldást.

[55] ITIL: Information Technology Infrastructure Library: Nemzetközileg elfogadott szerződéskötési ajánlás, amelyet speciálisan az informatikai szerződések és projektek lebonyolítására alakítottak ki. Egyaránt támogatja a Service Support és Service Delivery szolgáltatásokat, és a PRINCE módszertannal kiegészítve alkalmas IT projektek tervezésére és lebonyolítására is.

[56] Az ITIL Service Delivery eleme jelentése: Service Level Agreement – azaz szolgáltatási szint megállapodás, ebben definiáljuk a szolgáltatásrendelkezésre állást, ami viszont a szolgáltató TIER fokozatával behatárolt.

időket jelenti, és ha ezeket az **ISP**[57] (szolgáltató) nem tudja tartani, hát bizony nagyon komoly szankcióknak (kötbér, kártérítés, fővesztés…) néz elébe.

Joggal mondhatja a kedves olvasó, elég! Abbahagyom! Nem olvasom tovább! Már megint egy rövidítés!

Minek még egy valami, aminek nem látom sem az értelmét, sem a célját..

Mi is ez az **ITIL** és hogy jön a **mosónőkhöz, akik korán halnak**[58]?

[57] ISP: Internet Service Provider: Internet (IT) szolgáltató.
[58] József Attila, Anyám című verse kelt: 1931. január 6.

Az ITIL és a rendszerüzemeltetők, akik szintén korán halnak.

Aki már volt gyakorló rendszergazda, vagy valamilyen IT rendszer, felelős üzemeltetője, az tudja mekkora napi feszültség és stressz ez a munka.(Nem lennék meglepve, ha statisztika alátámasztaná, hogy a rendszergazdák tényleg korán halnak...)

Az informatikai szolgáltatási szerződések alapvetően, a polgári jog[59] hatálya alá tartoznak és a kötelmi jog tárgyalja és „rá lehet húzni" az egyes szerződések közül, többet is, de az ilyen típusú szerződések létrehozása nehéz feladat. Egyrészt lényeges informatikai ismereteket feltételez, másrészt ezeknek adekvát jogi megfeleltetést, vagy egyedi konstrukciókat kell hozzárendelni, mert ezek a szerződések a kötelmi jog rendszerében vegyes szerződések.[60]
Ez nem csak a magyar, hanem más jogrendszerekben is (pl.: az általam mélyebben ismert német jogban) jogi-megfogalmazási problémát[61] vetett fel.
Az informatikai szerződésekben keverednek a megbízási, eredménykötelmi, szolgáltatási elemek melyek érdemi és pontos elhatárolása a már fent vázolt nehézségekbe ütközik. Még problémásabb az érdemi **felelősség behatárolás** megfogalmazása.

Egy **valós és „egyszerű" szerződéskötési helyzet** példát véve alapul:

> Kössünk egy céget ellátó többoldalú szerződést, elkülönült vonalbérlettel, egy adatközpontban bérelt szerver eléréséhez, amin egy saját céges üzemviteli (**ERP**)[62] rendszert akarunk táveléréssel üzemeltetni, outsourcing -olt rendszergazdákkal, saját **LAN**[63] üzemeltető munkavállalókkal és a szerződésben ki akarunk térni a működés kiesés idejére vonatkozó kártérítési megállapodásokra.[64]

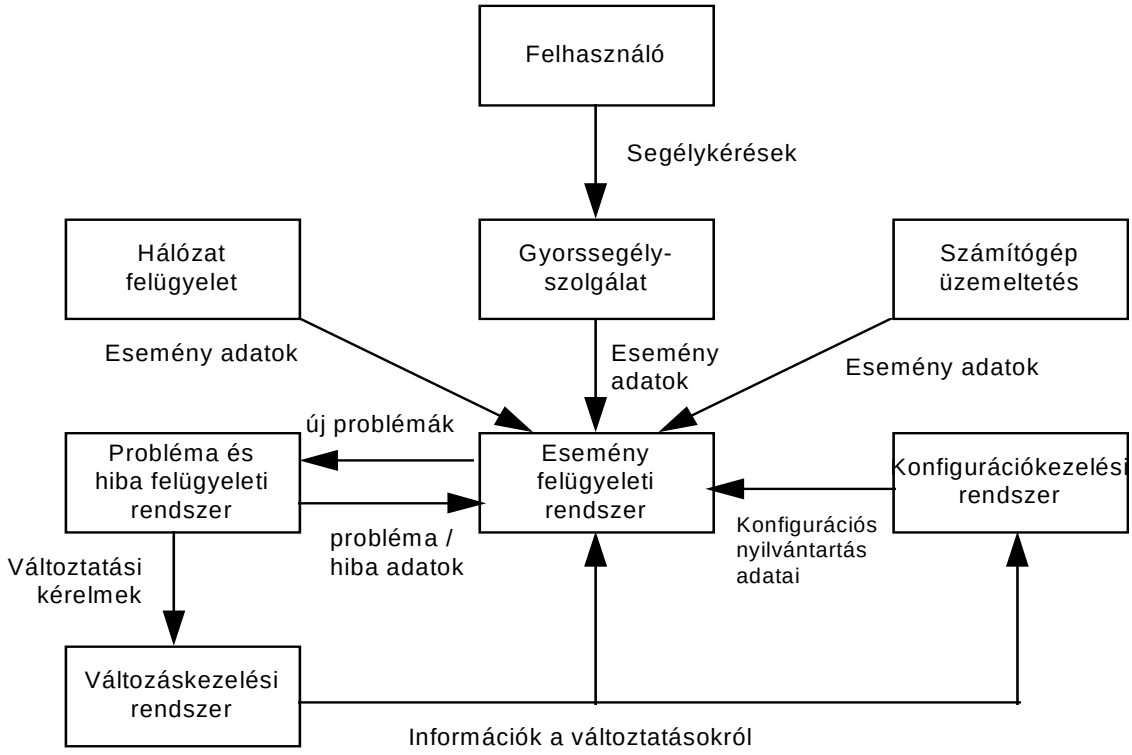
[59] Lásd: az 1959. IV törvény A Polgári Törvénykönyv Magyarázata, Közgazdasági és Jogi Kiadó 1992. Negyedik rész.
[60] Eörsi-Kemenes-Sárány-Világhy (1967): „Kötelmi Jog (különös rész)" Nemzeti Tankönyvkiadó 2002. 6. oldal.
[61] Német Polgári Törvénykönyv: Bürgerliches Gesetzbuch 55. Auflage 2004. im Buch 2. „Recht der Schuldverhältnisse" 241. oldaltól Kiadó: Deutsche Taschenbuch Verlag
[62] Enterprise Resource Planning -
[63] LAN: Local Area Network. Helyi hálózat:
Andrew S. Tannenbaum, Prentince Hall – PANEM 1999 Computer Networks. Third edition. 27. oldal
[64] A szerző már hozott létre, több ilyen és kiválóan működő ilyen szerződésrendszert.

Az **ITIL** tulajdonképpen egy egységes, rendszerszemléletben összeállított probléma megoldás halmaz (Library = könyvtár), amiket egy-egy informatikai szerződések (lehetnek akár projektek is) készítésekor a feleknek célszerű egymás között tisztázni illetve egyes problémák felléptekor az egymás között lefolytatandó eljárásokat rögzíti. Ennek segítségével, könnyebben tisztázhatjuk egy a fenti példa jogi kereteit.

Az ITIL v3[65] a szolgáltatások megalapozása (Service Support) sorozat öt részből áll (itt most a többi részre nem térek ki):

- konfigurációkezelés
- gyorssegélyszolgálat
- problémakezelés
- változáskezelés
- szoftver felügyelet

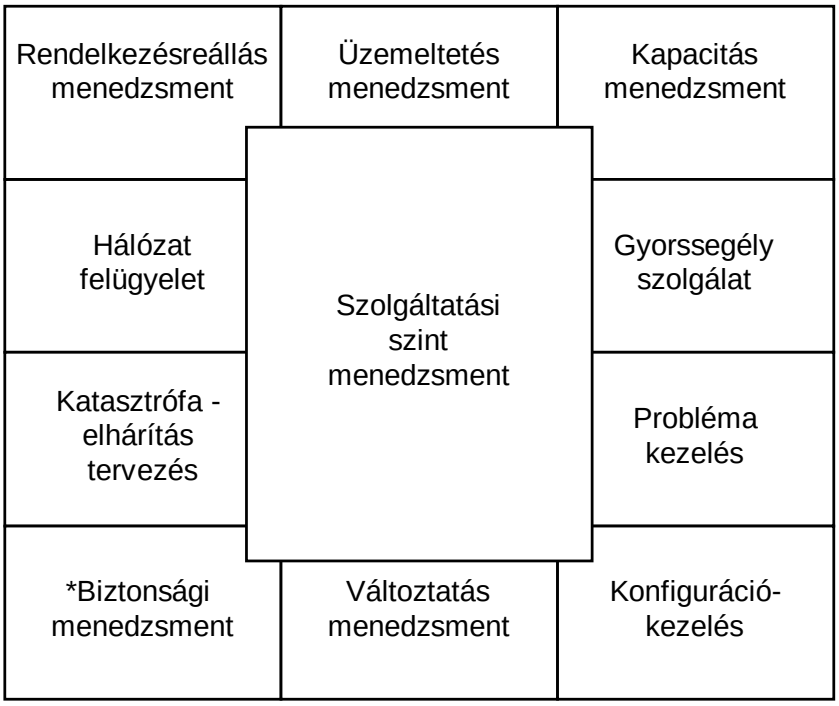
Ezeknek a szorosan összefonódó témáknak az integrálása vezet el a szolgáltatások megalapozásának a legfontosabb eleméhez: egy teljes körű változtatás-, probléma- és eseménykezelő rendszerhez.



1. ábra. Probléma és eseménykezelő rendszer

[65] ITB Információ Tárcaközi Bizottság ajánlása: Az 1999-ben Kormányzati forrásokból létrehozott és fenntartott „non governance" koordinációs bizottság, melynek célja az állami és privát szféra informatikai struktúrájának felépítése, javítása és belföldi, külföldi koordinációja.

A cél az, hogy gyakorlati útmutatást adjon egy ilyen rendszer felépítéséhez az ötlet fogantatásától a rendszer üzemeltetéséig és karbantartásáig, aminek során az ITIL egyes moduljait használjuk fel.



2. ábra. A szolgáltatási menedzsment részei

Visszatérve a megelőző „párnázás” – ra. Tehát erre már a beruházási koncepcióban, még a tervezési fázis előtt ki kell térni, mert alapvetően meghatározzák a tervezési programot és az üzleti koncepciót is.

A következőkben egy közreműködésemmel előkészített és általam tervezett valamint a kulcsrakész átadásig és a munkavállalók betanításáig lebonyolított beruházás keretében fogom bemutatni a fentiek értelmezését és külön kitérek a kapcsolódó biztonsági területekre is.

ESETTANULMÁNYOK:
TIER 1 IT (1993) ami valójában egy kétszeres hibatűrésű rendszer volt - bemutatása és javaslatok:

Amit itt elmondani és demonstrálni szeretnék, hogy az elmúlt évtizedek informatikai fejlődése, mely egybemosta a szervezés elmélet és módszertan kérdéseit az IT fejlesztés kérdéseivel.

Gyakorlatilag a szervezés elmélet az IT módszertan részévé vált, jóllehet az IT az csak egy lehetséges eszközmegoldás a szervezés támogatására.

Ezt mára teljesen elfeledtük, és ezzel megszűnt a racionalitás.

Az IT fejlődése egyben háttérbe szorította az emberi munkaerő alkalmazásának kérdéseit. Az IT fejlődése és biztonsága egyre több „feleslegesé" vált munkakört szüntetett meg, kiiktatta a rendszerek **más szervezési módszerekkel** történő biztosítását és mára paranoiás ISMS-é nőtte ki magát.

Nincs alternatív szervezési megoldásunk az elektronika helyett és ez az egész rendszer sérülékenységének az alapja. Nincs igazi két egymástól független párhuzamos N, nincs igazi 2N, pedig volt ilyen időszak, én még emlékszem rá és dolgoztam is benne. Sok munka volt vele, de nem volt paranoiánk. Persze, dolgozni kellet.

TIER 1, ami valójában egy igazi TIER 4 volt! 1993-ban egy jellegzetesen kisvállalkozás IT kidolgozása és felépítése, majd működtetése volt a feladatom. Ahol az informatika tulajdonképpen a papíralapú működést támogatta és mindkét rendszer a számítógép alapú és a kézi papír alapú feldolgozás párhuzamosan működött.

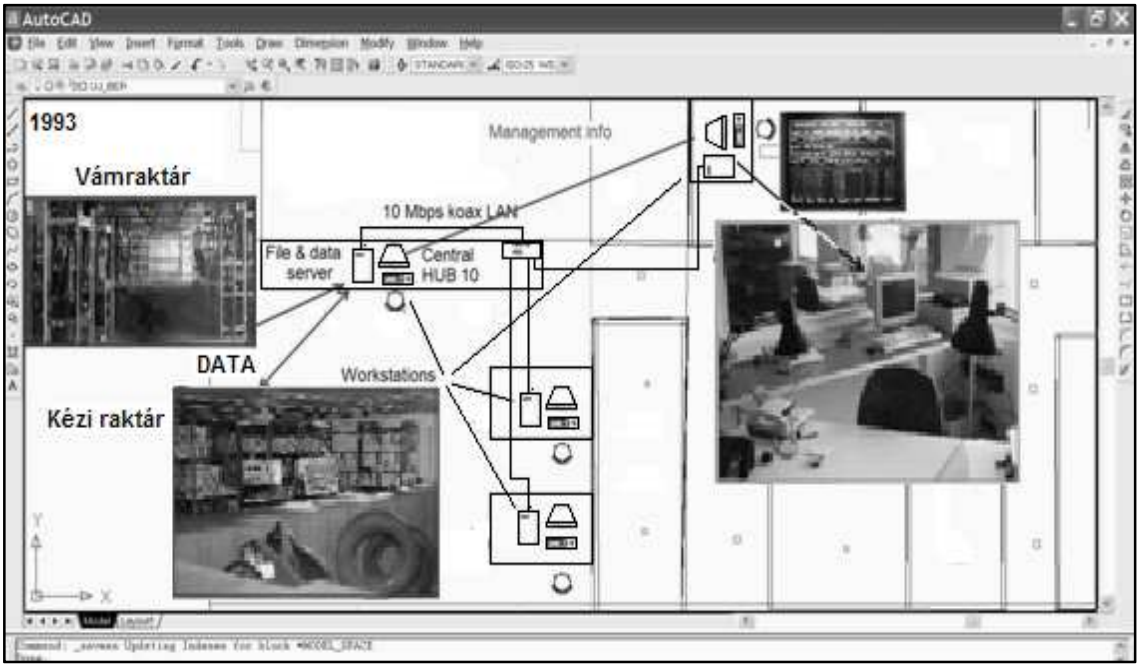
Maga az informatika a mai megközelítésben TIER 1, azaz egy nem redundáns rendszer volt, azonban az ezzel párhuzamosan működő másik rendszer a kézi kartonos feldolgozással együtt szervezés elméleti szempontból tekintve **kettős hibatűrésű rendszer**nek volt felfogható. Ezen el lehet vitatkozni, hogy ez most TIER3 vagy 4. DE valójában ezek a működések kettős hibatűrésűek voltak, ráadásul nagyon erősen

függetlenedni tudtak az elektromos ellátás és a **LAN** [66]zavaraitól, hiszen a kézi, papír alapú feldolgozás nappali világosság mellett még akkor is tudott üzemelni, ha az IT éppen üzemképtelen volt.

Ez azért lényeges, mert a redundanciának nem az IT, hanem IT-n kívüli más szervezési megoldás volt a hordozója: jellegzetesen a papír alapú táblázatos kinyomtatások, táblázatok és készletkartonok (printek). Ez mára elavultnak tűnik, de ez volt az igazi KÉT FÜGGETLEN PÁRHUZAMOSAN MŰKÖDŐ RENDSZER, AMELY ELTÉRŐ ENERGIAELLÁTÁSSAL MŰKÖDIK.

Hogy is nézett ez ki?

Ez volt az „informatikai rendszer” 1993-ban :



Mint látható nem volt IT redundancia. A **DOS illetve WIN for Workgroups 3.11** [67] és **UNIX** [68]alapú rendszerek, **Novell Net Ware 4.1**[69] és **10 Mbit/s koaxiális hálózat**[70], **DBASE IV adatbázis**[71] **kezelő**vel még

[66] LAN – Local Area Network, helyi számítógép hálózat
[67] A szerző 1989-ben SZÁMALK, „MS-DOS rendszerprogramozóknak” oklevelet szerzett
MS Windows for Workgroups 3.11, User Guide 1991, MICROSOFT Coprporation
MS-DOS 6.1 User Guide 1994, MICROSOFT Corporation
[68] A szerző 1989-ben SZÁMALK, „UNIX-XENIX” oklevelet szerzett
Kernighan & Pike: „A UNIX operációs rendszer” magyarul 1987, Műszaki Könyvkiadó
[69] Borges & Eisler: „PC-hálózat építés” magyarul, 1997 PANEM kiadó, 68., 151. oldal 4. fejezet
[70] Borges & Eisler: „PC-hálózat építés” magyarul, 1997 PANEM kiadó, 41. oldal RG 58 kábel
[71] Szlovák-Tóth- Kőri: „Adatbázis kezelés, programozás dBASE IV-ben” 1989, LSI, ATSZ, a PLUSZ kiadó

azt is jól bírta, ha – miként az gyakran megtörtént – kiment a volt TSZ ellátó hálózatából kapott elektromos áram. Ez volt az un. hőskorszak, aminek elhíresült Bill Gates mondása volt, „Kapcsold ki és be.” Ha nem működött a számítógép, akkor meg folytattuk manuálisan a munkát.

Ha a gépen tárolt adatok mentek tönkre, a készlettablókból egyrészt lehetett azonnal tovább dolgozni, másrész újra fel lehetett vinni az adatokat. Voltak napi adat mentések, azokból az előző napi adatokat vissza lehetett állítani, így a kézi pótlás, csak az aznapi bevét- kiadás bizonylatokra, meg számlákra korlátozódott.

Az IT berendezések magas ára miatt, nem volt informatikai hibatűrés, de volt helyette a manuális feldolgozás teljes második rendszere. KÉT teljes és egymástól teljesen független rendszer volt, jóllehet maga az IT csak **1xN** rendszerként üzemelt. (Az általam tervezett és kialakított rendszer kisvállalati rendszer volt, de hatalmas cégek is tudtak ilyen alapon működni.)

A kézi feldolgozás terén, később vehettünk (kaptunk az anyavállalattól) egy fénymásolót, így a kézi feldolgozás is N+1 rendszerűvé vált.

IT terén, pedig csak jóval később sikerült annyit elérnünk, hogy előbb a szerverhez, majd a munkahelyekhez vettünk **UPS**[72]-t. Így az elektromos ellátásra N+1 tartalék jött létre. Később a napi mentések bevezetésével az gépi adatállományokra még bejött az N+1. (legalábbis a napi backup.)

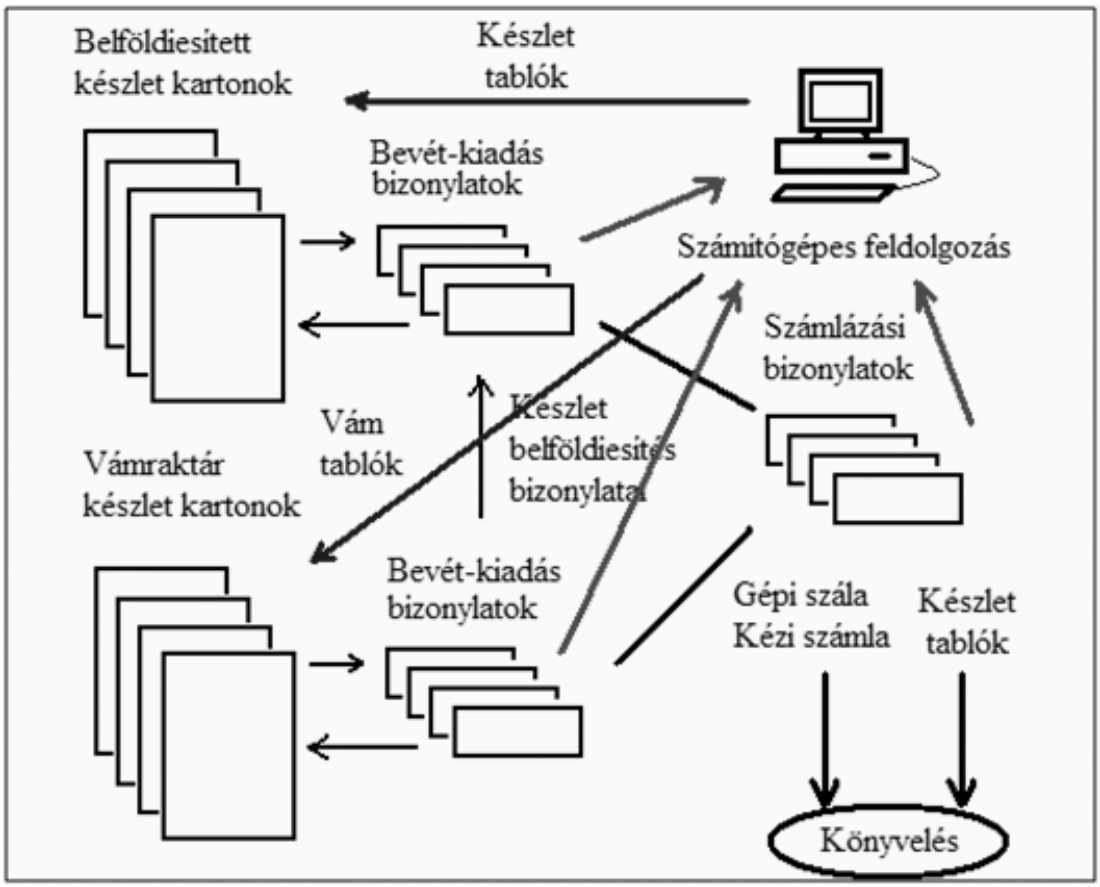
Ez már lényegesen biztonságosabb munkát biztosított. Áramkimaradás esetén, az UPS-ek mintegy 20 perc **áthidalási időt**[73] tettek lehetővé, így vagy helyre állt az áramszolgáltatás vagy ez alatt, jól lezárhatóvá (elmenthetővé) vált az addig végzett munka és a szervert valamint, a munkahelyeket rendben ki lehetett kapcsolni és el lehetett kezdeni a manuális munkát. Hozzá kell tennem, a „brutális” ki-be kapcsolások sem ártottak. Ezeket leginkább a monitorok nem szerették, könnyen

[72] Uninterrupted Power Supply: Szünetmentes tápegység. Áramkimaradás esetére az akkumulátora kapacitása mértékéig működteti a hozzákapcsolt számítógépeket és egyéb elektromos berendezéseket.
[73] Más néven kitartási időtartam: Az UPS által a ráterhelt berendezések működésének fenntartási idejét jelenti. Tartama függ az UPS háttér akkumulátor kapacitásától, a ráterhelt berendezések számától illetve ezek összesített energia felvételétől.

tönkrementek, de sem a hálózat sem maguk a számítógépek az adatbázisokkal, sem a mátrix printerek nem voltak ezekre érzékenyek.

A rendszer leállítási időt hívjuk **„shut down" időtartamnak**[74] illetve a tartalék rendszerre való átállás időtartamát **átkapcsolási időnek**[75]**.**

Ez volt a számítógépes feldolgozással támogatott kézi kartotékrendszer:



Az éves rendelkezésre állási idő, gyakorlatilag az év 365 napjából a ténylegesen dogozandó munkanapok munkaóráira korlátozódott. Ha volt is informatikai kiesés vagy hiba akár ez idő alatt is – azt szinte azonnal lehetett kézi feldolgozással is folytatni. Magyarán, akár volt áram és IT akár nem, tudtunk folyamatosan dolgozni.

[74] „SHUT DOWN" A rendszer leállításának folyamatát jelenti, melynek során lezárásra kerülnek a folyamtatban lévő hálózati tranzakciók, adatbázisok, hálózati kapcsolatok, felhasználói- és rendszer programok majd a folyamat lezárulva fizikailag is kikapcsolható a rendszer. (áramtalan állapotba hozható) A folyamat kezdetétől a sérülés mentes fizikai kikapcsolhatásig terjedő időtartamot nevezzük „SHUT DOWN IDŐTARTAM"-nak.

[75] Valamely redundáns rendszerben, a tartalékrendszerre való 100%-os átállásra való ideje.

Ez idő szerint még lehetett (persze a kellő kockázatot felmérve, és annak hatásait elkerülve) munkaidőn kívül az éles rendszeren egyes dolgokat kipróbálni, rendszert fejleszteni. Az ilyenre rendelkezésre állt pl. a pénteki zárástól a hétfő munkakezdési terjedő idő.

Amikor minden rendben működött, fel lehetett dolgozni a közben keletkezett adatokat naprakészre a számítógépes rendszeren.

Ha jobban belegondol az ember ez egy igazi TIER 4-es filozófiát valósított meg! **2 * (N+1)** kettős hibatűrés, két egymástó teljesen független rendszerrel.

Ja, majd' elfelejtettem. Jó sok ember dolgozott. Volt raktáros, raktárkönyvelő, pénztáros, kiadó, informatikus…

Ezután nézzük mi volt ezekkel kapcsolatban a már korábban összeírt kérdéseinkre az itt adható válasz?

Meddig tart a hálózat túlterhelése?
Októl függően, amíg olyan sok felhasználó volt, hogy a HUB broadcast üzenetei elvitték az adatforgalom jelentős részét, vagy amíg a meghibásodott HUB-ot, vagy hálózati eszközt, szakaszt nem azonosítom, és ki nem iktattam. Ez gyakorlatilag a teljes leállítást és a rendezett és rendben működő rendszerekkel történő teljes, vagy rész újra indítást jelentett.

Okozhat-e a túlterhelés károsodást a hardverben?
Gyakorlati tapasztalatom alapján, az ebbe és az ezekhez hasonló rendszerekben nem. Általában az ok-okozat fordított volt, előbb volt a hardver meghibásodása és ennek következménye lett a túlterhelődés.

Megnyomhatom-e ezt a piros gombot, amire az van írva „RESET"?
Hiba, hálózati hiba vagy géplefagyás esetén, szerveren, munkaállomáson gyakorlati tapasztalatom alapján igen meg lehetet nyomni. Sőt gyakran az egyetlen „javítási" mód volt. Persze nem örült neki senki, elvesztek az éppen végzett és el nem mentett munkák. (Ez azért komoly kár, szorozzuk csak be néhány a munkavállalók napi bérével…)

Hol van? Melyik?
HUB Ki kell húzni a teljes hálózatból és újra visszadugni mindent, vagy leállítani a hálózatot és újra indítani.
Szerver: Ez a gomb itt az elején.
Printer: Ki/Be gomb, vagy húzd ki.

Mi van, ha mindent gyorsan kikapcsolok?
Jó eséllyel, az aktuálisan végzett és el nem mentett munkákon kívül nagyobb bukfenc nélkül leáll minden. Használatban lévő dBASE IV állományok esetben felléphetnek **index állománysérülések**, de ezek helyreállítódnak a következő bekapcsolásnál, ha nem akkor kézzel újra kell definiálni, ha úgy se ment, akkor jól jönne egy **használható mentés**.(Kisvállalatnál vagyunk: **Van mentés? Használható?**)

Kikapcsolhatok mindent gyorsan?
Elvileg igen.

Mi a gyors?
Elvileg, ha mindenki egyszerre elkezdi a kikapcsolást 1-2 perc a munkaállomásokra, további 1-2 perc a szerverre. Ez azonban csak elvi érték. A **valós kikapcsolási időérték** ennek sokszorosa 15-20 perc.

Joggal vetődhet fel a kedves olvasóban a kérdés, mi értelme ezelőtt közel húsz évvel működött technikákat vizsgálni…?

Megsúgom az informatika lényege azóta sem változott, hogy **ilyen magas üzembiztonságú kettős hibatűrésű rendszereket üzemeltettünk** az informatikai őskorban.

A jelszó a költségcsökkentés volt – így jutottunk mára ide, ahol vagyunk, ma már szinte egy-egy informatikusra van „rálőcsölve” akkora informatikai érték, hogy ha még a származékos károkat is hozzáveszem [76] pestiesen szólva sok a jóból.

Jelen értekezésem néhány kulcskérdése már ebben az informatikai őskorban is megvolt és ez kihat a mai ISMS korábban tett javaslataimra.

Mi az, amit a mai informatika korában, alacsony költségráfordítással megtehetünk?

Az ISMS kapcsán tettem már javaslatot és ez a képzés szerepe. Nem az egyetemi vagy más tanfolyami képzésé, hanem a helyi rendszeren kell az azt üzemeltetőknek **VESZÉLYELEN gyakorlási, kipróbálási lehetőséget**

[76] Károk és elemzésüket lásd: Jelen tanulmány „Döntési modellek” 23. oldal címnél és a 28. oldalon.

valahogyan biztosítani. Ennek egyik olcsó lehetősége, ha az ember együtt nő fel az általa gondozott rendszerrel.

Továbbá egy barátom szava járásával, „Kell egy homokozó, ahol veszélytelenül mindent ki lehet próbálni és be lehet gyakorolni, mielőtt kimész a sivatagba."

Mit is kell tudni kipróbálni?
A legegyszerűbbel kezdem: az adat **állományok és a rendszerek mentése**. Ezek a mai informatikában rutin feladatoknak tűnnek, egészen addig, amíg egyszer nem fut le rendesen a mentés és azt nem észleljük.(Mondhatnák ilyen nincs, pedig azt mondom még a számomra megismert legkorszerűbb mentési rendszerekkel is találkoztam látszólag, jó, rendben lefutott, de valójában visszaállításra alkalmatlan hibás mentéssel.)
A legalapvetőbb minimális teszt, a **mentések visszatölthetőségének ellenőrzése**. Működik-e amit visszatöltünk, vagy vissza fogunk tölteni. Persze ez is költségkérdés, nincs rá idő és nincs rá +1 szerver a kipróbálásra, éles rendszeren meg nem kísérletezünk…

Aztán ennek folyományaként jönnek a rendszer **upgrade -** k[77]. És itt ugorjunk időben a mába: Hányszor találkoztam az éjjeli automatikus biztonsági frissítés után reggel a cégbe beérve, lefagyott és nem üzemelő rendszerrel… És itt nincs +1 vagy 2N !

Hibásan futott le a frissítés. Az nem működik, amit napi szinten használunk. Áll a gyár. Nincs anyagkiadás, nincs munkalap, nincs beszerzés…

Áll a termelés. (*Bocsika' mondja Bill, majd kiadunk egy* ***patchet***[78] *és lőn' már pár nap múlva letölthető… „valahol egy honlapon, egy messzi-messzi szerveren…"*)

Mit tehet egy ilyen helyzetben egy informatikus?

Hibát keres, újra telepít, újra indít. Minden perc számít.

[77] Operációs rendszerfrissítés. Régi verziót, egy újabb verzió rátelepítése váltja fel.
[78] Szoftvergyártók által, rendszerhibák, vagy javítások hibáinak utólagos kijavítására kiadott javító programocskák, amiket manuálisan kell lefuttatni.

MEGINT ITT AZ IDŐFAKTOR:
Mit is írtam az előző oldalakon?

1/ **„A gyorsaság nem kirobbanás, hanem kompozíció”**
Tizenöt év edzés, gyakorlás és 30 másodperc a bizonyításra ez az arány…

2/ „Gyorsan kell dönteni, mert hatékonyabbnak és gyorsabbnak kell lennie a védekezésnek, helyreállításnak, mint az okozott kár eszkalációja előrehaladásának.”
Ha nincs kellő gyakorlás, nem kompozíció lesz, hanem összeomlás…

Ugorjunk időben és nézzünk egy a mai szemmel már korszerűnek tűnő (általam) tervezett, kiviteleztetett illetve részben általam épített rendszert amelyben már teret kapott a TIA 942, ISMS, ITIL és rácsodálkozunk az ERP-re, ahogy az pénzt csinál!

ERP rendszer upgrade 2007, előtte kis kitérővel.

Mielőtt e tényleges feladat ismertetésre áttérnénk, ismerkedjünk meg, nagyvonalakban az ERP rendszerekkel. Ez azért fontos, mivel a korszerű vállalatirányítás elengedhetetlen eleme az ERP. Számos ilyen rendszer ismert a legáltalánosabban ismert talán az **SAP**[79], de kisebb jelentőségűeket lehetne **még tucatszám**[80] felsorolni.

Az általam itt ismertetetésre kerülő (általános) modell jellegzetes. Lényegi elemei megtalálhatóak – különböző megoldásbeli eltérésekkel – mindegyik **globalizálódott** rendszerben.

Lényegük, hogy ezek olyan, a vállalati **üzleti folyamatokat** tervezni, követni és irányítani képes felhasználói szoftverek, amelyek egyben megoldják az ezzel kapcsolatos adatállományok tárolását is és képesek – multinacionális cégek – interkontinentális munkafolyamatait is kezelni. Hasonló elven működnek az informatikára és **interkontinentális hálózatok**ra alapozott börzék is, amelyek fejlődése és „pénztermelése" volt az elmúlt évtizedek informatikai fejlődésének fő motorja.
Nézzük milyen is ez a rendszer fő alapjaiban.

Cseppben a tenger, avagy a bitben a globalizáció.

Globalizálódott rendszer?

Az adattárolás alapegysége a bit – amely egy „igen" vagy „nem" jelet jelent. A kettes számrendszerben számol 1 vagy 0 értéke lehet. Egy alfabetikus betű leírására a kezdetben 8 bitet használtunk fel. Hogy milyen jelsorozatokhoz, milyen jelentést értsd: betű vagy számkaraktert, vagy egyéb jelet (jelentést) rendelünk, az megállapodás kérdése.

Ezeket szabványok tartalmazzák, ilyen például az **ASCII**[81] 8 bites szabványa, amelyet az IBM fejlesztett ki az 1960-as években és az angol

[79] SAP: **SAP AG** 1972-ben alakult Németországban, eredeti neve „Systemanalyse und Programmentwicklung", aminek jelentése „rendszerelemzés és programfejlesztés". A rövidítését később átértelmezték, az új „Systeme, Anwendungen und Produkte in der Datenverarbeitung" név jelentése: Rendszerek, alkalmazások és termékek az adatfeldolgozásban.
[80] EPICOR, MIS, IFS...
[81] Forrás: Klaus Dembowski, „PC táblázatok" Kossuth kiadó 1997. 15. oldal

ABC összes kis és nagybetűjét, a görög ABC egyes betűit valamint a képernyőn rajzolásra alkalmas jeleket (256 db) tartalmaz.
Például az „A” betű ANSI 8 bites ábrázolása (jelsorozata) 0001 0100 ezt egyszerűbben két hexadecimális számmal szoktuk jelölni, akként hogy az első és a második négy bitet ($2x2^4$ = 2x16) egy-egy a 16-os számrendszerbeli számmal fejezzük ki. Jelen példánknál maradva: az A betű ANSI jele: „#14” a szám elé tett „#” jel azt mutatja, hogy ez egy 16-os számrendszerbeli ábrázolás, amely az ANSI táblázat 65. karakterét jelenti azaz „A” betű.

Később, a globalizáció hatására, hogy más nyelvek egyedi írásjelei is megjeleníthetőek legyenek létrejött egy **UNICODE**[82] (rövidítve UCS – kód) nevű szabvány, amely már képes a világ nyelvkaraktereit leírni.

Ez a szabvány már 32 biten ábrázol és minden egyes UCS – kód a maga 32 bitjével egy-egy (karakter) pozíciót jelöl ki, ami 2 147 483 647 (azaz 2^{31}-en szám) féle jel, vagy karakter megjelenítésére alkalmas, tehát az **UCS – kóddal leírhatók többek között a japán és kínai írás (távol-keleti nyelvek) ékírásjelei is**.

No, itt a globalizáció a bitekben…

Az előző részben tárgyaltam, egy 1993-as párhuzamos számítástechnikai és kézi adatfeldolgozás rendszer leírását, mint kettős biztonságú rendszert.

Nem túl nagy adatmennyiség volt egy ekkora cég életében. Napi néhány kilobyte, amit még párhuzamosan két egymástól teljesen független és eltérő szervezés megoldású rendszerben is kezelni tudtunk. Hozzáteszem az anyavállalat és a magyarországi telephely közötti a számítógépen rögzített adatok, már láthatóak voltak mindkét helyen, egy Data Link[83] telefonvonalon keresztül továbbítva.

[82] Forrás: Klaus Dembowski, „PC táblázatok” Kossuth kiadó 1997. 17. oldaltól 1.5-1.6 fejezetek
[83] Telefonvonalon bonyolított adatkapcsolat két távoli számítógép kötzött.

Ha az információ alapegységét bitnek tekintjük, akkor a legegyszerűbb leírásban egy karakter az 8 bit[84] Az ANSII karakter rendszerben 1 byte amit egy karakternek nevezünk az egy betű.
Az adatmennyiséget azzal jelöljük, hogy hány byte, azaz mennyi a digitális formában leírt, tárolt vagy továbbított karakterek száma. Itt már ismerős szavakkal találkozunk: „Megabyte”, „Gigabyte”…
Ezek a mai világunkban köznapi fogalomként, kézzelfogható adatmennyiségeket jelölnek.
Ha DVD-t veszünk, azt fejből tudjuk, hogy az 4,2 Gbyte (gigabyte) vagy hogy egy CD lemezre 720 Mbyte azaz 720 megabyte fér. Jóllehet az igazi összefüggéseket talán nem is tudjuk. (Minek az elv, ha valami kézzelfogható?)

Az alábbi **táblázat**ban[85] a bit-byte-kilobyte-megabayte… egymáshoz kapcsolódó váltószámait láthatjuk. Mivel kettesalapú számrendszerből eredve használjuk rájuk a tízes számrendszerbeli százas, ezres váltószám fogalmakat némi eltérés van közöttük, így adódik, hogy 1 kilobyte az 1024 byte. (És nem pedig 1000.)

ÁLTALÁNOS MEGÁLLAPODÁSOK ÉS SZOKVÁNYOK

1 bájt = 8 bit
1 kbájt = 1024 bájt
1 Mbájt = 1024 kbájt = 1 048 576 bájt
1 Gbájt = 1024 Mbájt = 1 073 741 824 bájt
1 Tbájt = 1024*1 Gbájt = 1024*1024 Mbájt

1.4. táblázat. Példák kettes számrendszerbeli számábrázolásokra

Ez az oldal amit Ön most olvas, a pályázati kiírás szerint oldalanként 32 sor és soronként 64 leütést (karakter) tartalmazhat (A betűköz – space – is karakter) **azaz egy oldalon 2048 betű van legépelve.** (ANSII karakterrel számolva, ez ugyan nem ismeri a magyar ékezetes betűket!)

[84] Mára már 32, illetve 64 bites rendszerekről beszélünk.
[85] Forrás: Klaus Dembowski, „PC táblázatok” Kossuth kiadó 1997. 9. oldal

Nézzük, hogy jön az adóbevallás a söralátétre?

Egy oldal: 2048 x 8 bit (1 byte) = 16.384 Byte
ami jó közelítéssel, kerekítve
(1000-el osztok, szorzok csak azért is) : 16 Kbyte
A tanulmány 40 oldalas az 40 x 16 = 640 Kbyte

Ez nagyjából egyenlő 10 db, terjedelmesebb SZJA adóbevallás adattartalmával.

Ha Magyarország 5 millió SZJA[86] adóbevallását számoljuk, akkor az:
(5.000.000 x 0,64 Mbyte) / 100 = 320 Gigabyte[87] adat egy évben.

Ez a mai adathordozók tekintetében egy kisebb méretű merevlemeznek felel meg, amely fizikai méreteit tekintve a tenyérnyi méret kategóriában van. (**Egy adóbevallás REKORD formában valóban ráfér egy söralátétre.**)

Ebben a méretben az adat, bizony eléggé mobilizálható valami, aminek védelme és itt a fizikai **elvitel** (SIC!) elleni, védelmet is értem, **adminisztratív-felelősségi rendszer** [88] betartására van bízva, ami mára ISMS – el is kiegészült.

Az adatlopások a jellegzetesen **látens bűnözés**[89] körébe tartozóak elég, ha csak a közelmúlt „Google Street View" városfényképező és közben biztonsági veszélyeket rejtő, adatgyűjtő[90] tevékenységét említem. (DE nem ez tanulmányom tárgya.)

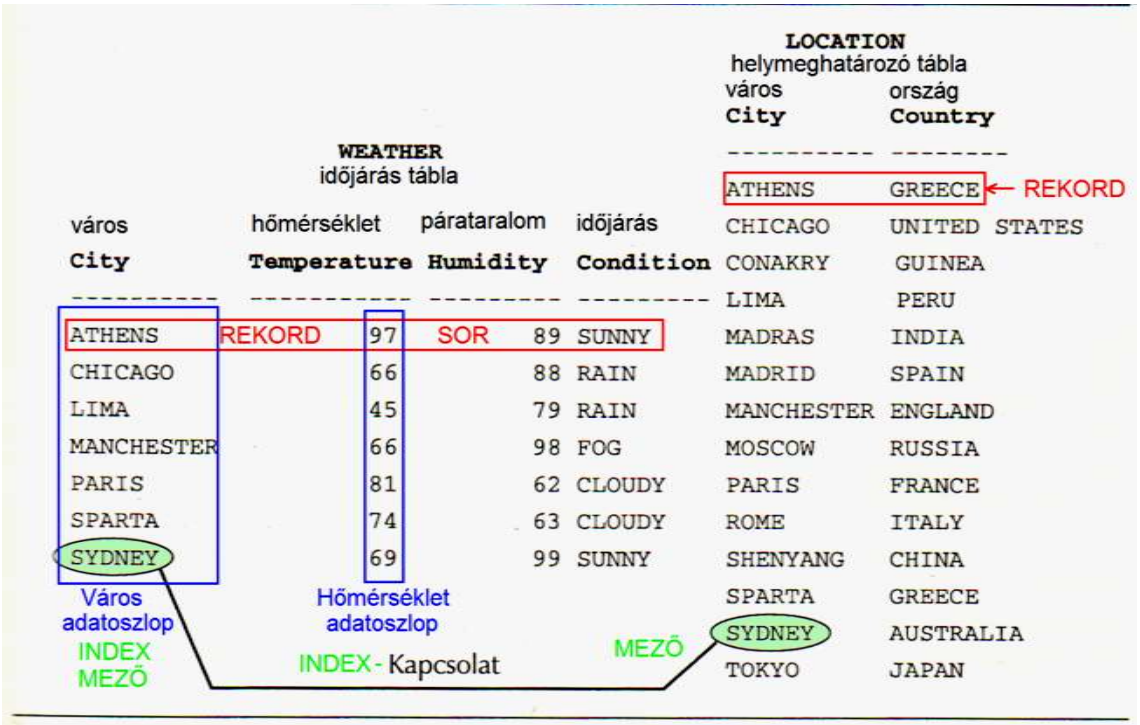
Az adatfeldolgozás keretében, az egy összefüggő adatsort nevezünk egy rekordnak. Egy rekord több mezőből áll, ilyen pl. az adózó neve, címe,

[86] Személyi Jövedelem Adó
[87] Az egyszerűség miatt mindenhol mellőzöm a 1024-es váltás használatát, helyette 1000-et használok.(A szerző)
[88] Forrás: A Szerzőnek a Legfőbb Ügyészség egyik pályázatán, a Legfőbb Ügyész különdíját nyert pályaműve.
[89] Göncöl-Korinek-Lévai: „Kriminológiai ismeretek, bűnözés, bűnözés kontroll" 1999 CORVINA kiadó Prof. Dr. Korinek László: A látens bűnözésről.
[90] Forrás: http://www.dailymail.co.uk/news/article-1259162/Google-Street-View-shows-secret-SAS-base-major-security-breach.html

adószáma. Egymás alá tartozó azonos típusú mezők a tábla oszlopok és ezek egységes állománya a relációs adatbázis[91]

Az **Oracle**[92] definícióját átvéve: A relációs adatbázis kezelő rendszer[93], egy olyan szoftver, amely általános célú adatok tárolását és visszakeresését teszi lehetővé úgy, hogy az adatokat táblákba szervezi és ezek olyan egy vagy több információs egységet (sort) tartalmaznak, amelyek ugyanolyan típusú adattételekből (oszlopokból) állnak. Az Oracle egy relációs adatbázis kezelő rendszer. Nézzük az alábbi szemléltető ábrát[94] :

Amelyet a könnyebb érthetőség miatt kiegészítő keretekkel és színezett magyar felirattal láttam el.



4.5. ábra. A WEATHER és LOCATION táblák közötti kapcsolat

A fenti tábla példának, jó. Azt mutatja, ha van egy helyi időjárás táblánk és van egy ország táblánk, és mindkettő tartalmazza a KAPCSOLÓ MEZŐ –

[91] Relációs adatbázisok.
Forrás: Szlovák-Tóth- Kőri: „Adatbázis kezelés, programozás dBASE IV-ben” 1989, LSI, ATSZ, a PLUSZ kiadó I kötet 1.6 cím, 26. oldal.

[92] ORACLE: Az **Oracle Corporation** a világ legnagyobb üzleti szoftvermegoldásokat kínáló cége, melyet 1977-ben alapítottak Kaliforniában. 1986. március 15-én, közel egy évtizeddel megalapítását követően az Oracle első, 2,1 millió darabos, nyilvánosan jegyezhető részvénycsomagjával megjelent a NASDAQ-on.
Forrás: oracle.com / FAQ

[93] Forrás: Kevin LONEY, ORACLE DATABASE 10g – Teljes referencia kézikönyv, 2006 PANEM kiadó, 1327. oldal.

[94] Forrás: K.LONEY, ORACLE DATABASE 10g – Teljes referencia kézikönyv, 2006 PANEM kiadó, 26. oldal.

ként használható VÁROSNÉV mezőket, akkor a két táblából egy virtuális **külső tábla**[95] képezhető, amelyik kiegészült az ország nevekkel.

Hát, ez meg minek? Nem jó semmire.
Kit érdekel, hogy a napos Sydney, Ausztráliában van?

De ha az alábbi három tőzsdéről vannak egyidejű adataim. Akkor az adott tőzsdéken szereplő részvényének árfolyama között teremthetek azonnali kapcsolatot.

Itt a pénz, ami az elmúlt évtizedekben az informatika fejlődését biztosította!

A TŐZSDÉK.

Tegyük fel, van a három tőzsdén egy-egy táblám, amiben soronként vannak az aktuális részvény árfolyamok, és oszloponként tudom vizsgálni, mennyi volt adott részvényem (ez lesz majd az KAPCSOLÓ mező) nyitó illetve záró árfolyama.
Tegyük fel, hogy van interkontinentális kapcsolatom az ezeket a táblákat kezelő számítógépek között. (Van SATELIT kapcsolat)
Tegyük fel, hogy van egy olyan virtuális tábla, amely tartalmazza a RÉSZVÉNY neve kapcsoló indexhez tartozó NYITÓ-ZÁRÓ részvényárfolyamokat
Tegyük fel, hogy van egy bróker, aki bekapcsolja az irodai számítógépét és ezeket az adatokat egyszerre látja.

Mit csinál ezekkel az adatokkal? PÉNZT. Annyi pénzt, amennyit akar.

Ahogy a föld forog, bezár a londoni tőzsde (létrejön a záróár) de nyit a new yorki tőzsde, ha elég gyors az interkontinentális adatforgalom, már látom az előző napi részvényárfolyam mozgásokat és azok figyelembe vételével tudok dönteni mit, adjak-vegyek, és amikor felkel a nap Tokyoban, már ez előző teljes üzleti nap árfolyammozgásait látva lehet: „make money” – pénzt csinálni.

No, nézzünk ezt az érdekesebb példát, a következő oldalon, hogyan is kell „make money” azaz pénzt csinálni egy relációs adatbázis kezelővel:

[95] Forrás: K.LONEY, ORACLE DATABASE 10g – Teljes referencia kézikönyv, 2006 PANEM kiadó, 21. oldal

Ime, a táblák, és a külső táblánk, a RÉSZVÉNY kapcsoló mezővel[96]:

LONDON

RÉSZVÉNY	NYITÓ ÁR	ZÁRÓ ÁR
BIKA részvény	100	115
Részvény 1	15	25
Részvény 2	1005	1100
Részvény 3	500	505
Részvény 4	480	444
MEDVE részvény	100	70

NEW YORK

RÉSZVÉNY	NYITÓ ÁR	ZÁRÓ ÁR
BIKA részvény	105	200
Részvény 1	25	25
Részvény 2	1005	1200
Részvény 3	500	480
Részvény 4	410	450
MEDVE részvény	90	60

TOKYO

RÉSZVÉNY	NYITÓ ÁR	ZÁRÓ ÁR
BIKA részvény	80	?
Részvény 1	18	
Részvény 2	800	
Részvény 3	480	
Részvény 4	500	
MEDVE részvény	95	

EGYSÍTETT VIRTUÁLIS TÁBLA NY CITY GMT 24:00 H

RÉSZVÉNY	LONDON	NEW YORK	TOKYO	TIME
BIKA részvény	115	200	vegyél	GMT 24:00 H
MEDVE részvény	70	60	adj el	GMT 24:00 H

Ha van egy ilyen relációs adatbázis kezelő interkontinentális rendszerem, akkor a tokyoi tőzsde nyitásakor, gyorsan-gyorsan veszek (80-ért) BIKA részvényt, mert az már NYC – ben 200-on zárt, és még reggel kapkodva eladok MEDVE részvényt, mert itt még kapok érte talán 95-öt, de NYC-ben már csak 60-at ér.

Stresszes élet a bróker élet. Lehet, hogy a brókerek is korán halnak?

[96] Forrás: K.LONEY, ORACLE DATABASE 10g – Teljes referencia kézikönyv, 2006 PANEM kiadó, 64. oldal.

A probléma, csak egy:

EZ A PÉNZ TEREMT PÉNZT RENDSZER ELSZAKADT A VALÓS GAZDASÁGI FOLYAMATOKTÓL. NINCS ÁRÚFEDEZETE. ADDIG KÉPES MŰKÖDNI AMÍG CSAK KEVESET KÖLTENEK VALÓS REÁLIÁKRA BELŐLE, MERT HA EZ A PÉNZTÖMEG MEGLÓDUL VÁSÁROLNI, ÚGY NEM LESZ ÁRÚFEDEZETE.

A MEGLÓDULT PÉNZTÖMEG ADDIG INFLÁLÓDIK, AMÍG ÉRTÉKE NEM TALÁLKOZIK A TÉNYLEGESEN RENDELKEZÉSRE ÁLLÓ ÁRÚFEDEZETTEL.

AZ NYER, AKINEK TÖBB PÉNZE VOLT AZ ÖSSZEOMLÁSKOR.

Térjünk vissza a 2007-es ERP upgrade projektre, mely egy közel TIER 3-as rendszer kiépítését jelentette. Ennek áttekintése azért hasznos, mert ez is számos kis, apró, de hasznos tanácsot adhat, mit is kellene csinálni, ha valami Kritikus Infrastruktúra összeomlás jönne.

Az ilyen és ehhez hasonló rendszerek, már ISMS szemléletben és TIA 942 biztonság szerint épülnek fel. Az Oracle, Windowsos környezetben, mint adatbázis motor működik egy nagy biztonságú szerveren.

A biztonság tekintetében, most csak az általam installált INTEL alapú szervert illetve rendszert ismertetném. TIA 942 szerint 2N biztonságú **INTEL**[97] DUO Core processzor, és a 2(N+1) biztonságú **RAID**[98] 10 merevlemez ellátás.

A RAID 10 sajátossága, hogy egyrészt jelenti a RAID 0 sorolásrendszer gyorsaságát, másrészt a RAID 1 tükrözéses technikájának köszönhető kettős hibatűrést, amelyet összesen négy merevlemezzel állítunk elő. A kettős hibatűrés és RAID a műszaki megoldása miatt, a meghibásodott merevlemezt menet közben egyszerűen ki lehet húzni és cserélni, nem kell a szervert leállítani.

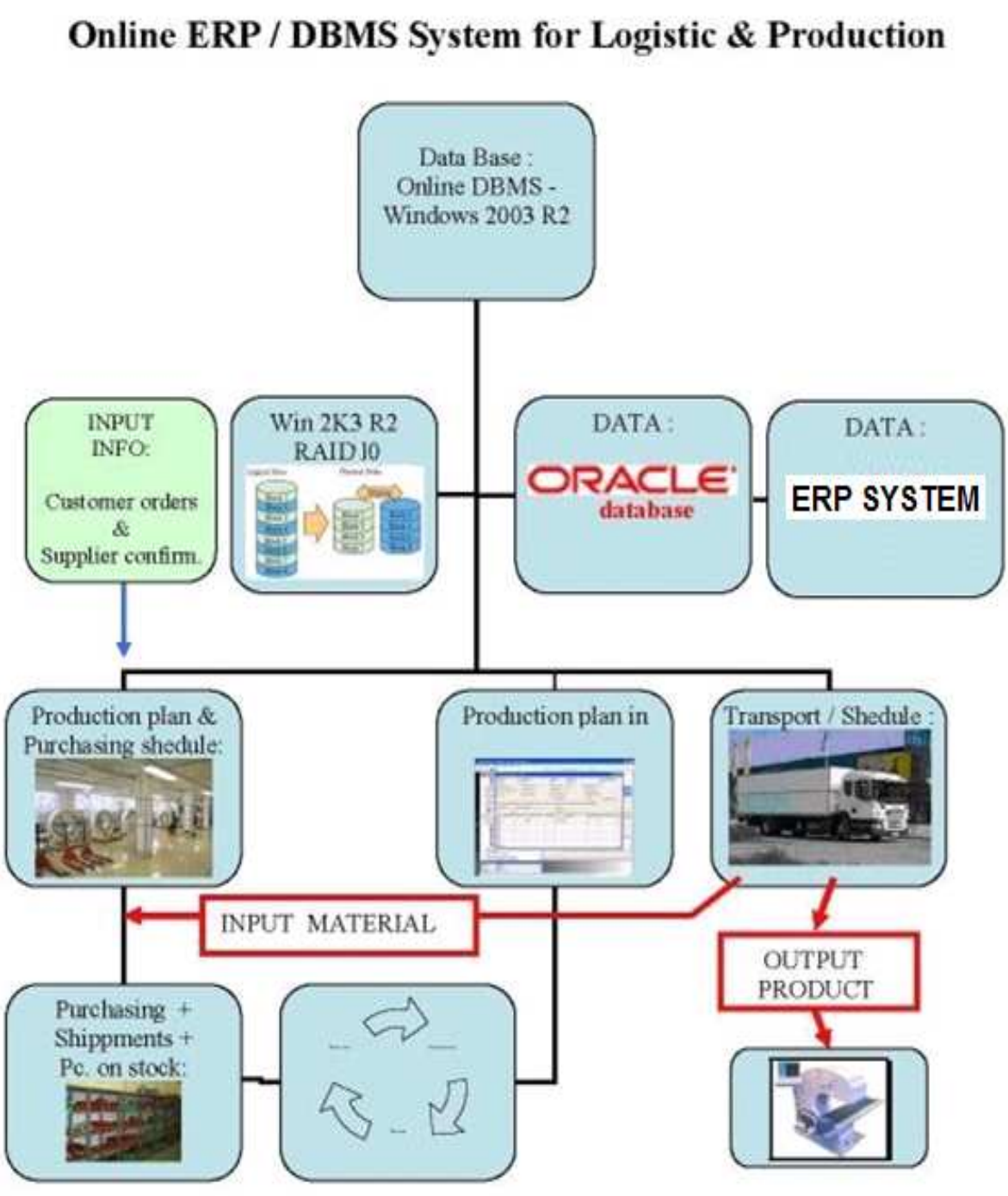
Az általam kialakított rendszert, ezen felül +1 redundánsra terveztük +1–1 tartalék merevlemez van a RAID-en felül.

Menet közben cserélhető a **BLADE**[99] szerver saját szellőzése is. Maga a szerverház ezek elérése céljából menetközben nyitható.

[97] Forrás: http://www.intel.com/content/www/us/en/search.html?keyword=INTEL+history AZ INTEL a világ, vezető multinacionális, processzor, és hardver gyártó cége. **INT**egrated **EL**ektronics mozaikszóból származik az elnevezése. A NASDAQ - ra bevezetett cég.

[98] Forrás: http://searchstorage.techtarget.com/definition/RAID: Redundant Array of Independent Disks. Független merevlemezek, redundáns környezete.

[99] BLADE (penge), un keskeny RACK szekrénybe helyezhető, ezért nagy adat és energia sűrűségű adatközpontok kiépítésére alkalmas szerverek. Korábban az un. main frame rendszerek (nagygépes) rendszerekkel ellentétben, a BLADE rendszer, kompakt, moduláris és gyártói szinten csereszabatosak.

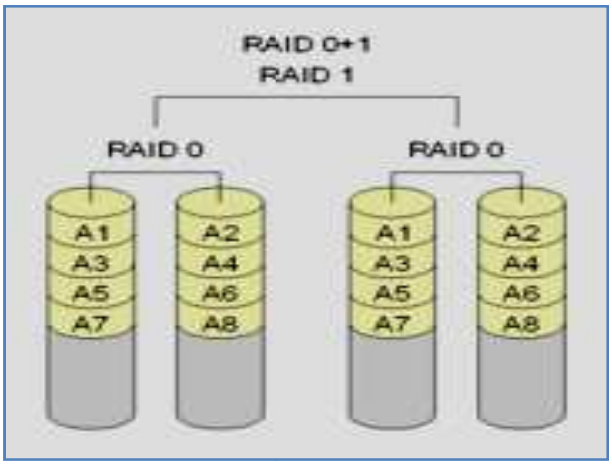


A fenti ábrán a szerző által összeállított rendszerséma látható.

Az adatbázis a RAID 10 kapcsolatában az alábbi:

1. kép: A szerver felülnézeti (demo) képe

2. kép: A szerver a szerelt RAID és merevlemez együttessel a szerelőasztalomon illetve a RAID struktúra.



A fentiek adják az adatbázis kezelő hardver alapját. Ez kiegészült egy N+1 biztonságú TRIPLITE 5000 VA táv menedzselhető UPS – el és egy fázis átkapcsolóval.

Ezzel a megoldással, ha csak egy fázis ment el, úgy lehetőség volt a másik fázisra átkapcsolásra illetve az UPS-el mintegy 30 perc rendszer kitartási időt tudtunk elérni, amelyet a helyben szokásos (SIC!) rendszeres, 5-10 perces áramkimaradások áthidalására elegendő volt. Ez a teljes rendszer shut down-ra is lehetőséget adott még úgy is, hogyha egyes bennragadt **USER**[100] – eket kézzel egyenként kellett kiléptetni.

A LAN helyi hálózat 2N biztonságú volt, a kulcsfelhasználók LAN és párhuzamos **WIFI** [101] elérést és saját UPS – t is kaptak. A switch – eket a szerver UPS – ről tápláltuk meg. A szerverszoba hűtése N+1 volt, de figyelembe vettük, hogy a szerverszoba hőterhelése nem érte el az
1 Kw/m2-t, tehát a természetes szellőzés, mint N elegendő volt a +1 a nyári meleg hűtésre kellett.

A rendszer szoftver a **Windows 2003 R2** [102] volt, amelyre adatbázis motornak az ORACLE lett telepítve és arra települt rá az ERP (IFS) rendszer.

A 2007-es ERP upgrade tapasztalatai, leszűrhető tanulságok.

A mentések tekintetében a rendszerszoftverek egy partícióba kerültek, így ezt elkülönülten lehetett menteni és külön partícióban voltak az adatbázis állományok és még ettől is elkülönítve a céges tervezői adat és rajz állományok. Bármelyik külön-külön menthető és visszatölthető volt.

A mentések visszatölthetőségét csak a telepítést követően a rendszerteszt során egyszer volt módunk ellenőrizni. Az éles rendszeren nem.

Átmeneti megtehető intézkedések voltak, huzamosabb áramkimaradás esetére ISMS szerint:

- Raktári kiadás és bevétel manuális könyvelése
- Kézi munkautasítások kiadása
- Folyó megrendelések kiadása és kézi könyvelése ERP rendszeren kívül
- MNB napi árfolyamok kézi rögzítése

[100] USER: Számítógép hálózatba bejelentkezett felhasználó.
[101] WIFI: vezeték nélküli mikrohullámú kommunikációt (WLAN) megvalósító, széleskörűen elterjedt szabvány (IEEE 802.11)
[102] MICROSOFT NT alapú szervermegoldás továbbfejlesztett változata: WINDOWS SERVER 2003 R2

Nem lehetett kiváltani kézi megoldással:

- Kiszállítás számlázása
- Kiszállítási csomagjegyzék és rakodójegy kiállítása

Tartós pár napos áramkimaradást még, gyártással és a fenti manuális szervezési megoldásokkal meg lehetett oldani, de ezen túl már leállt a termelés.(Ilyenre nem került sor, a leghosszabb áramkimaradásunk egy napos volt, egy transzformátor leégése miatt.)
Kábelfektetési munkák miatt egyszer volt egy betervezett két napos leállásunk, de az csak kisebb indulási problémákkal járt.
Villámcsapás miatt megsérült a bejövő internet CISCO hálózati egység, cserélni kellett.

Egy 2011-es banki esettanulmány, sok tanulsággal.
Banküzemi informatika,[103] az igazi motorja az IT fejlesztéseknek és üzembiztonságnak. Egy általam idén megismert felülvizsgálat tapasztalatai jól mutatják, hogy milyen megtehető költséghatékony intézkedések is lehetnek.
Az alapproblémát, annak vizsgálata jelentette, hogy egy áramkimaradás esetén meddig tartható fenn a banki informatika működése.

Több dolog került vizsgálatra:
Áramkimaradás esetén:

- IT klíma fenntartás
- IT berendezések üzem fenntartása
- Épület klíma és a Facility működés (kiléptetés, liftek…)fenntartása

Az IT klíma fenntartás bár bizonyos szintig rugalmasnak tűnik, mert rendszerüzemeltető szemmel ez a kezdetben csak úgy jelentkezik, hogy meleg van a szerver teremben. Látszólag nem nagy probléma, de csak egy pontig. Itt visszautalnék a 2007-es ERP rendszer szerverére. Ennek olyan háromszintű belső hő védelme van. Az első szint a saját belső hűtőventillátorok hűtési teljesítményének növelése és rendszergazdai értesítés küldése. Ha ez kapacitásilag kimerült és a szerver hőmérséklet tovább emelkedik, úgy rendszergazdai riasztás küldése, végül rendszer shut-down a hardver fizikai károsodásának megelőzésére.

Áramkimaradás esetére történő tervezés esetén, milyen IT és Facility területeket és milyen szempontokat célszerű végig gondolni?

Célszerű:

- A vészhelyzetben figyelembe veendő (fenntartandó) eszközök és fogyasztók pontos és teljesítmény szerinti összesítése.
- IT és mellékrendszereinek redundancia és hibatűrés meghatározása
- Ezeknek, mint tervezési céloknak a meghatározása az UPS, aggregátor és tartalék áram betáp figyelembevétele szempontjából.
- IT vészhelyzeti intézkedések (ISMS)
- Épület és kapcsolódó facility vészhelyzeti intézkedések

Az alábbiakban egy általános vázlatot ismertetek, amely azért a tanulságokat is tartalmazza:

[103] Szerző a tárgyban csak az általános tapasztalatokra hívhatja fel a figyelmet, mert a konkrét tárgyban banki titoktartási nyilatkozat köti.

Havaria áramkimaradás IT és Facility tervezése:

Első lépcső (rövid áramkimaradás 1-2 perc):
UPS-ekre átkapcsolás – szerverek áramellátása folyamatos

Tervezési szempont:

- IT és Facility javaslat a szükséges energiára, hibatűrésre és redundanciára.
- Fenntartandó **berendezések és fogyasztási** adataik
- Szerverek, háttértárak, egyéb berendezések
- Közvetlen klíma berendezések és egységeik

Második lépcső (hosszabb 3-20 perc áramszünet):
IT UPS-ek kitartási értékeinek vizsgálata – szerverek áramellátása folyamatos

Tervezési szempont:

- IT és Facility javaslat a szükséges energiára, hibatűrésre és redundanciára.
- Fenntartandó **berendezések és fogyasztási** adataik
- Szerverek, háttértárak, egyéb berendezések
- Közvetlen klíma berendezések és egységeik
- Shut-down folyamat pontos feltérképezése benne
  + Munkafolyamatok és távoli adatelérések (fiókhálózat) lezárási időtartama
  + Rendszer leállítás időtartama

Facility intézkedések – liftek kiürítése, lezárása lépcsők használata

Tervezési szempont:

- Az átmeneti működés fenntartása és az esetleges épület kiürítés lehetőségének előkészítése.
- Tartalék árambetápra (tartalék fázisra) átkapcsolás (ha van 2N)

Harmadik lépcső (hosszú 20 percet meghaladó áramszünet):

IT tartalék aggregátor(ok) kitartási és ellátási teljesítményeinek vizsgálata.

Tervezési szempont – szerverek működése folyamatos:

- IT és Facility javaslat a szükséges energiára, hibatűrésre és redundanciára.
- Fenntartandó **berendezések és fogyasztási** adataik
- Szerverek, háttértárak, egyéb berendezések
- Közvetlen klíma berendezések és egységeik
- Shut-down folyamat pontos feltérképezése benne
  + Munkafolyamatok és távoli adatelérések (fiókhálózat) lezárási időtartama
  + Rendszer leállítás időtartama
- Shut-down döntés meghozatalának utolsó időpontja

Facility intézkedések – liftek kiürítése, lezárása lépcsők használata, vészkijáratok és kijárati útvonalak megnyitása.

Tervezési szempont:

- Az átmeneti működés fenntartása és az épület kiürítés, műszaki és fizikai feltételeinek megteremtése.
- Tartalék aggregátorok és vészhelyzeti energia ellátás időtartama és energia igényének felmérése az evakuálási terv függvényében.

Negyedik lépcső (teljes leállás és épület kiürítés):

IT intézkedések műszaki feltételeinek megteremtése

Tervezési szempont:

- Shut-down döntés meghozása és végrehajtása
- Rendszerleállítási folyamatok definiálása
- Egyéb megteendő intézkedések
- IT személyzet épület elhagyási terve (ha szükséges)

Facility intézkedések:

Tervezési szempont:

- Épület kiürítés és vészhelyzeti személyzet ellátásának műszaki feltételeinek kialakítása
- Tartalék aggregátorok vészhelyzeti üzemelése a hátramaradó személyzet függvényében.

Egy TEIR 3-at meghaladó moduláris kiépítettségű adatközpont beruházás 2011-es beruházói igény összefoglalója kapcsán tett javaslataim az utolsó, általam ezen, tanulmányban bemutatásra szánt téma:
sok tanulsággal.

Itt vissza kell utalnom az itt már korábban tárgyalt, az előkészítés fontosságára utaló részekre.

Milyen az előkészítési fázisban megtehető intézkedéseket javasoltam, és ezek miként köszöntek vissza az elkészült tervekben?

Infrastrukturális és Közmű tervezett és általam javasolt egyeztetései:

- **TIA 942-es szabvány TIER 3 és TIER 4 értelmezése jelen pályázati kiírásra.**
- Úthálózat (Gyalogos, gépjármű közút, kerékpárút és ipari teherbírású utak)
- Vasúthálózat illetve ipari vágánykapcsolat
- Fentiekhez kapcsolódó gépkocsi és kerékpár parkolók rendszere
- Szennyvíz csatornahálózat és kapcsolódó létesítményei
- Felszíni csapadék és csurgalékvíz elvezetés hálózat
- Felszíni közcélú víztározó létesítmények (köztó, víztározó, tüzivíz)
- Vízhálózat: (ivóvíz, lakósági szürke víz, mezőgazdasági és ipari célú víz, tüzivíz - ez 4 hálózat)
- **Katasztrófavédelemi egyeztetés a kritikus infrastruktúra védelem kapcsán**
- **Telefonhálózat és kapcsolódó berendezései**
- **Internet gerinchálózat és bekötése az országos hálózatba**
- **Mobil telefonhálózat és kapcsolódó létesítményei**
- **Elektromos nagyfeszültségű hálózat és kapcsolódó létesítményei illetve bekötése az országos hálózat (ok) ba** 2*(N+1) (?)
- Elektromos alacsonyfeszültségű (400 V) helyi hálózat és kapcsolódó létesítményei (transzformátorok, aggregátorok, UPS.)
- **Földgáz közmű hálózat és kapcsolódó létesítményei**
- Távhő szolgáltatás nyújtására kiépített hálózat (DC hulladékhő hasznosítás)
- Földfelszín alatti létesítmények – gáz, gázolaj és víztárolók

Mint a fenti listából kijelöltek két nagy kérdéskört tárgyalnak:

- TELCO
- Energiaellátás

Ebből a jelenlegi állapot szerint, az energetikai koncepciót tudom – hasonló titoktartási nyilatkozat hatálya alatt – elsősorban tapasztalati általánosság szinten összefoglalni.

Az elektromos ellátás szempontjából a leglényegesebb a teljes kiépítettségű adatközpont és üzemeltetési épület összes energia igényének a meghatározása.

A szervertermek alapterületét teljes kiépítettségben vegyük 1000 m2-nek
Az átlagos teljesítmény mutatót tekintsük: 1 KW/m2
Legyen az elérendő lokális maximum 10 KW/m2.
Számított energia a szerverekre: 1000 KW = 1 Megawatt
Kiegészítő létesítményekre: + 20 % = 1,2 Megawatt
Redundancia: + 20 % = 1,4 Megawatt

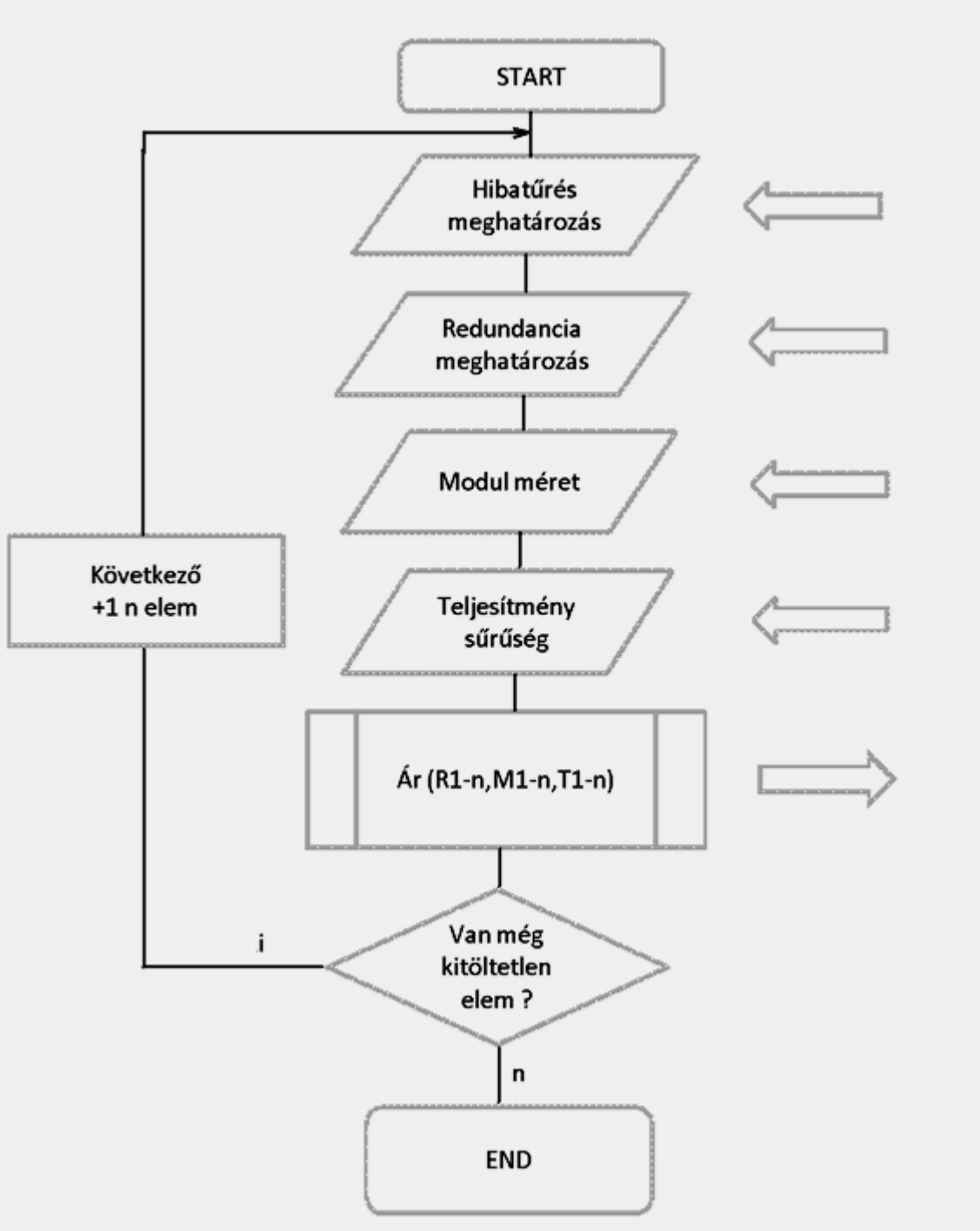
Hogy az egész rendszer milyen szinten kerül TIER 3 vagy TIER 4 besorolásba, úgy ennek kialakulásának menetét az alábbi folyamatábrával tudom szemléltetni. Látható, hogy az előkészítési fázisban megfogalmazásra kerülő koncepciók egy-egy árazott (költségvetés szinten: várható becsült bekerülési költség) alapon többféle hibatűrés és különböző tartalékkal készülnek. Tehát variábilisak. Ezek variációk között (és ezzel természetesen értendő a bekerülési ár változásai is) egy 3 változójú függvény[104] írja le, melyet egyszerűbben mátrixként írhatunk le. Így került a függvény megoldás helyett általam kidolgozásra egy 3 dimenziós változó mátrix amely:

- egyik változója a hibatűrés és redundancia,
- másik változója a modulméret
- harmadik változója a teljesítmény sűrűség.

Az ezen, változó elemekhez rendelünk egy-egy bekerülési értéket és ebben a formában már alkalmas a műszaki tartalom egyszerű definíciójára és ezáltal, a jogi (szerződéses) használtara.

[104] A többváltozós függvény ötletének kitalálója a beruházás CTO vezetője volt, míg magam a függvénynek a mátrixá alakítását és ezzel szerződésbe ültethetőségét dolgoztam ki.

A beruházó ezen, mátrix elemei közül a rendelkezésre álló erőforrás függvény figyelembevételével és az üzleti terv várható bevételi prognózisai alapján hozza meg a beruházási döntést.
Maga a beruházás műszaki tartalma és az ár összevetése egy iteráló eljárással jön létre az alábbiak szerint.



Tehát ez az, az egyeztetési eljárási folyamat, amelynek eredményeként létrejön az üzleti, cégérték nyereség szempontjából megtehető előzetes

megelőzések köre. Ráadásul, ez ebben a formában úgy jön létre, hogy azt egyszerűen lehet egy tervezői szerződésbe átemelni, mint műszaki tartalmat.
A bonyolultság problémáját érzékeltetendő, nézzünk egy lényegesen egyszerűsített példát, csak egy változó mentén mozogva vizsgáljuk a bekerülési költséget:

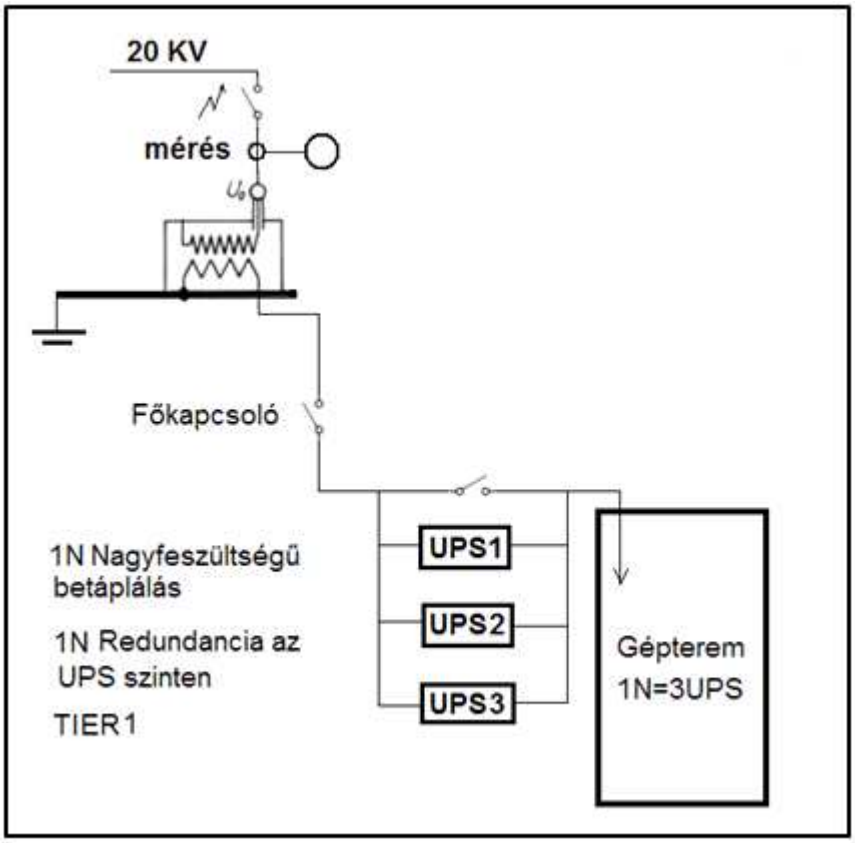
Nézzük a TIER fokozat változásai szerinti műszaki tartalmat és az árat csak az elektromos rendszerre:

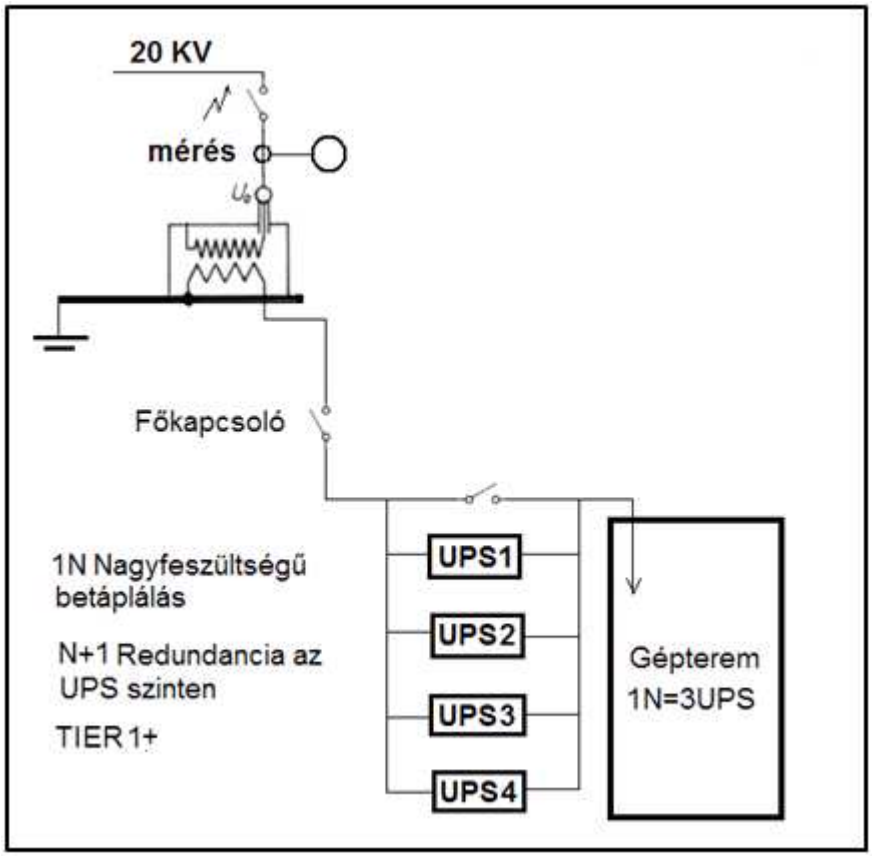
A bekerülési árat csak ilyen egyszerűen számítom:
Diesel aggregátor: 1000 /db
Transzformátor: 500 /db
UPS: 100 /db
Automata átkapcsoló e példában itt, most nem számolok vele
Kábelezés e példában itt, most nem számolok vele

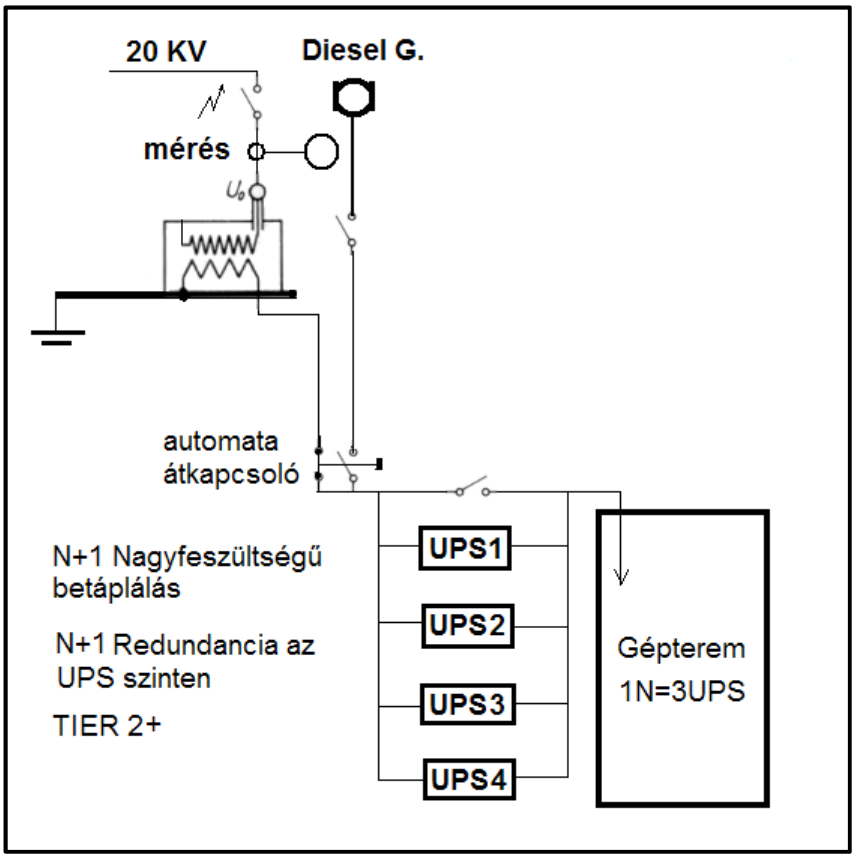
BIZT.	TRAFÓ		AGGREGÁT		UPS		ÖSSZ ÁR	SZORZÓ
FOK.	db	Ár	db	Ár	db	Ár		
TIER1	1	500	0	1000	3	100	800,00 Ft	1,00
TIER1+	1	500	0	1000	4	100	900,00 Ft	1,13
TIER2	1	500	1	1000	4	100	1 900,00 Ft	2,38
TIER3-	1	500	1	1000	8	100	2 300,00 Ft	2,88
TIER3+	2	500	1	1000	8	100	2 800,00 Ft	3,50
TIER4-	2	500	2	1000	8	100	3 800,00 Ft	4,75

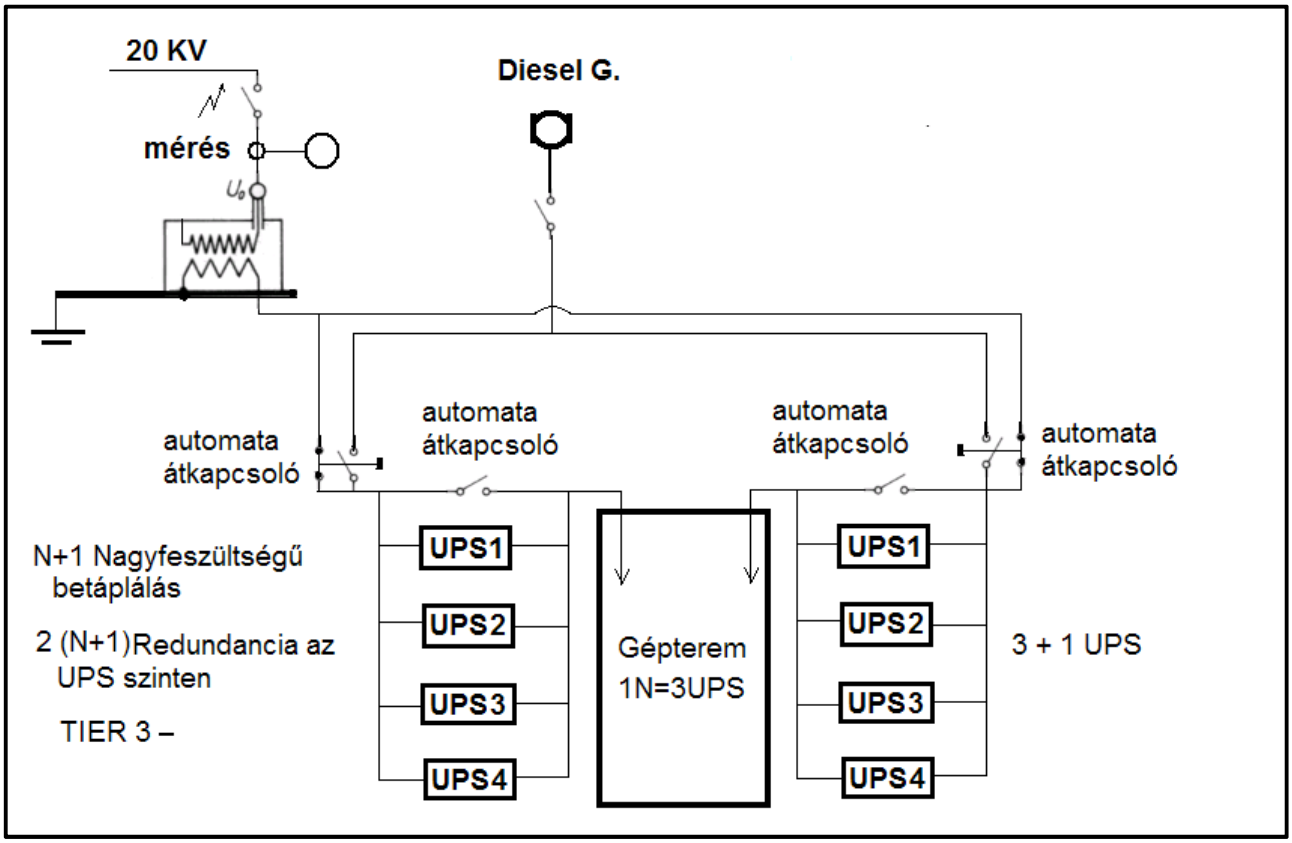
Ha hozzáteszem az általam készített vonalas „tervrajzokat”, látható, hogy már a beruházás előkészítési fázisában, nagyon széles mozgásterünk van a szükséges biztonsági fokozat és a megelőzési költségfüggvény valamint a rendelkezésre álló források összevetésére.
Természetesen az itt felvázolt elektromos rendszer csak egy eleme a teljes beruházás összköltségének, hasonló megoldással lehet feldolgozni a klíma, hűtés és fűtésrendszer, egyéb gépészet és az építészet területeteket.

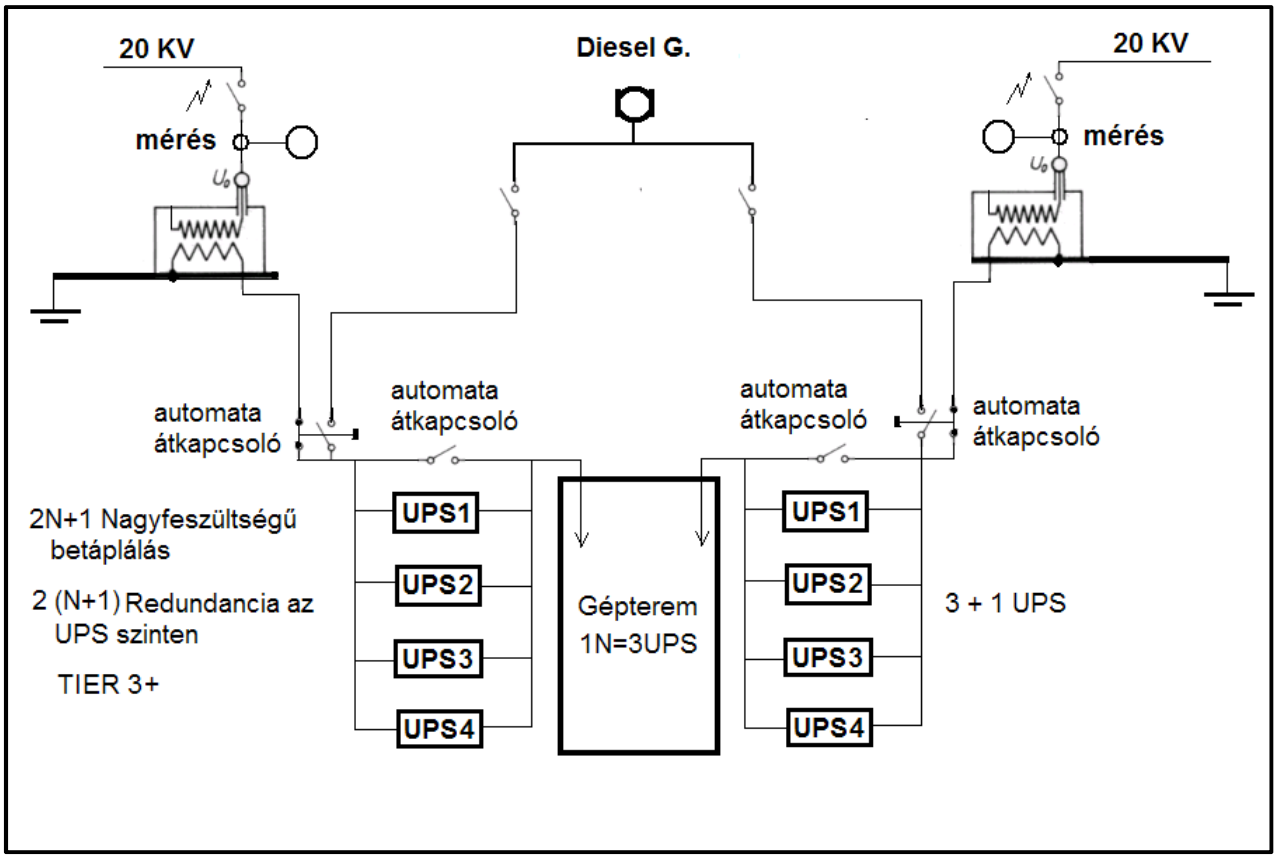
A következő oldalakon a TIER fokozatokhoz kapcsolható egy-egy elektromos műszaki megoldás látható, korántsem a teljesség igényével.

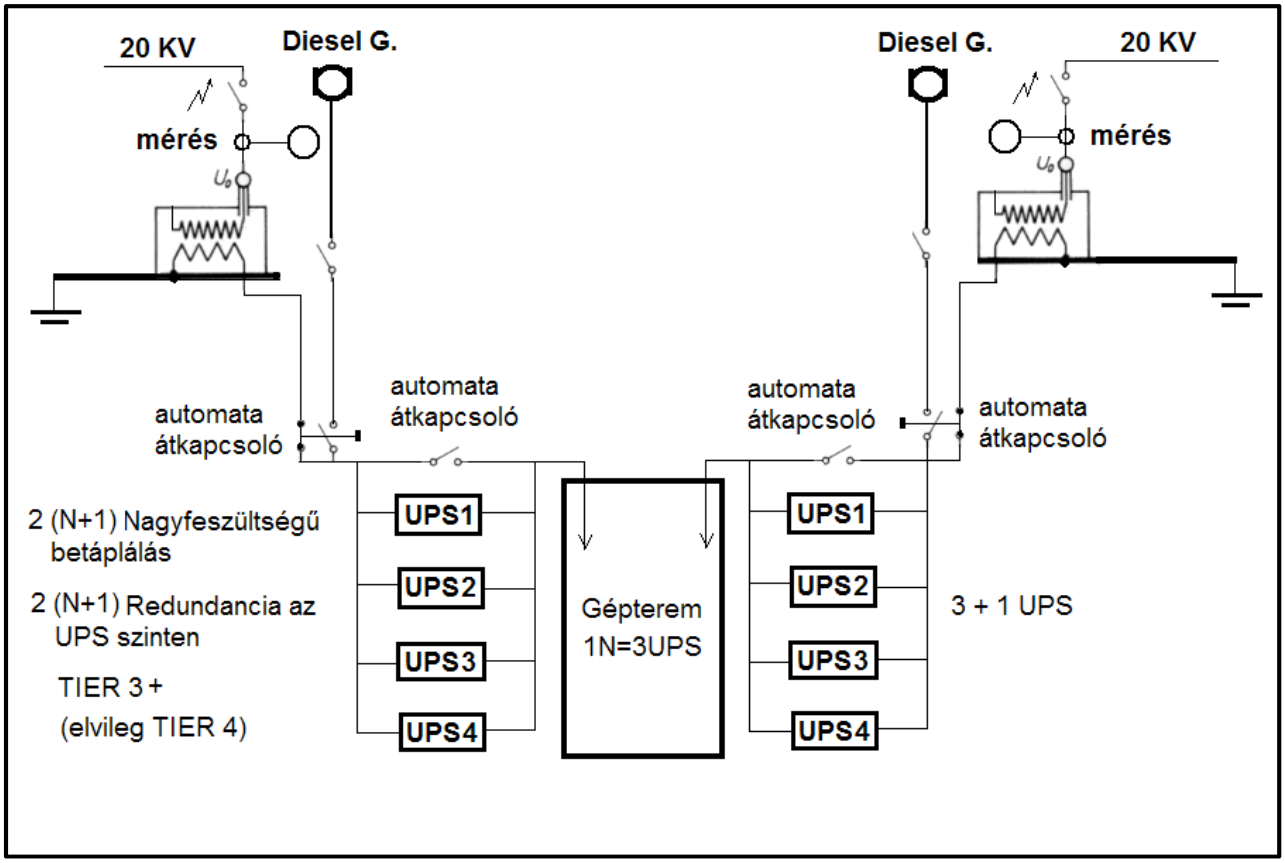

20 KV
mérés
Főkapcsoló
1N Nagyfeszültségű betáplálás
1N Redundancia az UPS szinten
TIER1
UPS1
UPS2
UPS3
Gépterem
1N=3UPS


20 KV
mérés
Főkapcsoló
1N Nagyfeszültségű betáplálás
N+1 Redundancia az UPS szinten
TIER1+
UPS1
UPS2
UPS3
UPS4
Gépterem
1N=3UPS


20 KV
Diesel G.
mérés
automata
átkapcsoló
N+1 Nagyfeszültségű
betáplálás
N+1 Redundancia az
UPS szinten
TIER 2+
UPS1
UPS2
UPS3
UPS4
Gépterem
1N=3UPS


20 KV
Diesel G.
mérés
automata
átkapcsoló
automata
átkapcsoló
automata
átkapcsoló
automata
átkapcsoló
N+1 Nagyfeszültségű
betáplálás
2 (N+1)Redundancia az
UPS szinten
TIER 3 –
UPS1
UPS2
UPS3
UPS4
Gépterem
1N=3UPS
UPS1
UPS2
UPS3
UPS4
3 + 1 UPS


20 KV
Diesel G.
20 KV
mérés
mérés
automata átkapcsoló
automata átkapcsoló
automata átkapcsoló
automata átkapcsoló
2N+1 Nagyfeszültségű betáplálás
2 (N+1) Redundancia az UPS szinten
TIER 3+
UPS1
UPS2
UPS3
UPS4
Gépterem 1N=3UPS
UPS1
UPS2
UPS3
UPS4
3 + 1 UPS


20 KV
Diesel G.
Diesel G.
20 KV
mérés
mérés
automata átkapcsoló
automata átkapcsoló
automata átkapcsoló
automata átkapcsoló
2 (N+1) Nagyfeszültségű betáplálás
2 (N+1) Redundancia az UPS szinten
TIER 3 +
(elvileg TIER 4)
UPS1
UPS2
UPS3
UPS4
Gépterem 1N=3UPS
UPS1
UPS2
UPS3
UPS4
3 + 1 UPS

Mi van a nappal?

Süt. Süt, mint mindig.

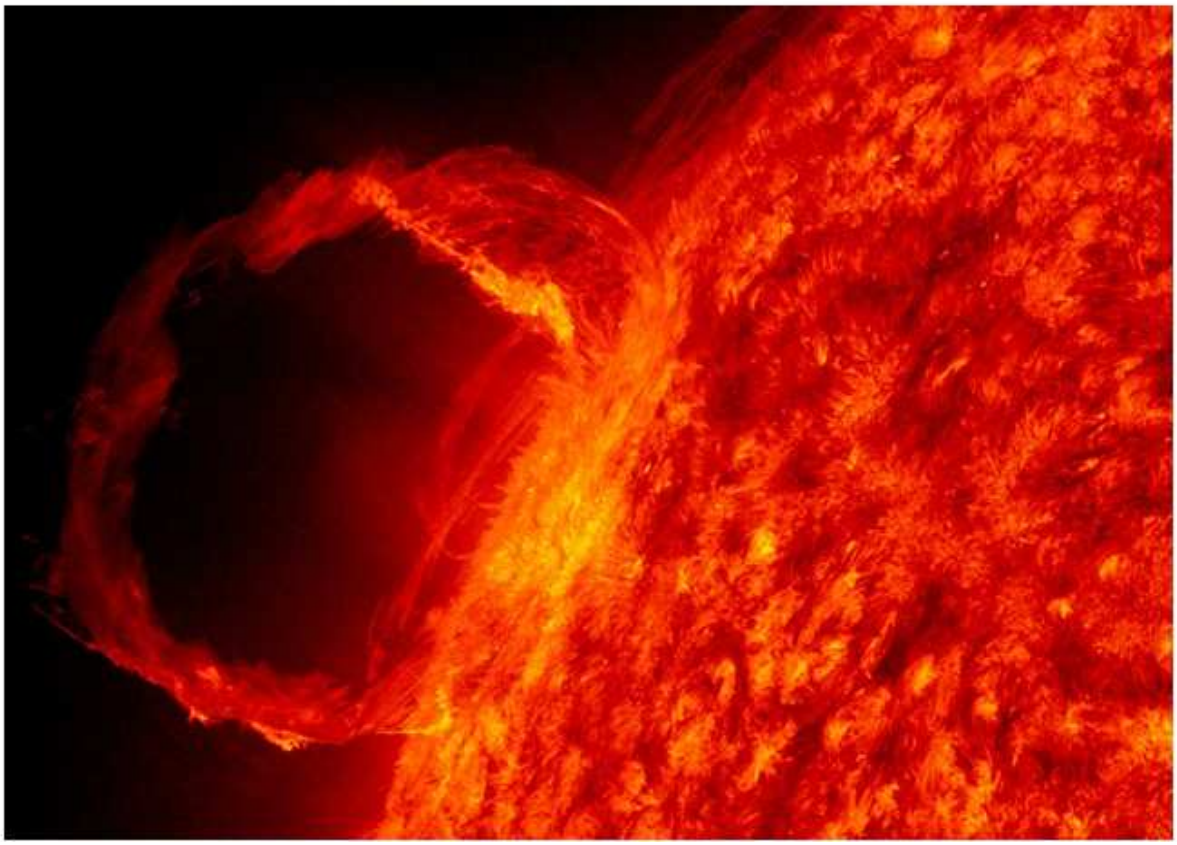
Ennek azonban vannak olyan, utólagosan felismert felmerülhető veszélyei, amelyek az előző évtizedek űr- és kapcsolódó beruházásai előkészítési fázisában mint tervezési szempont nem merültek fel.

Az elmúlt évtizedek űrforradalma és vele párhuzamosan a földi létesítmények kialakítása olyan tervezési szempontok szerint történt, mely a beruházások üzleti érték modelljére (lásd: jelen tanulmány 24. oldal.) alapozó hibatűrés és előzetes megelőzési költség szemléletben készültek, azaz nem számoltak azzal a felértékelődéssel, amit az informatika mára elért.

Az ORIGO hírportálon[105] megjelent ismertetés szerint:

Várhatók-e nagy napkitörések és ezzel kapcsolatos veszélyek 2012-ben?

A naptevékenység 11 éves ciklus szerint változik, és a maximumok környékén mindig erősebb aktivitás, nap- és koronakitörés jellemző. Csillagunk aktivitása főleg a műholdas távközlést és helyzetmeghatározást veszélyezteti, amire próbálnak is felkészülni a szakemberek a rendszerek fejlesztésével. Erős naptevékenység lesz jellemző 2012 és 2014 között végig, de nem várható semmilyen extra esemény kifejezetten 2012-ben.



[105] Forrás: http://www.origo.hu/tudomany/20110919-vilagvege-2012ben-az-igazsag-niburu-planetx-napkitores-polusvaltas-becsapodas.html

A képhez tartotó szöveg egy bulvár hír, a lakósági tájékoztatás része. De valamit többet takar, ha nem vagyunk felkészülve távközlési és energetikai rendszereinknek védelmére, olyan behatások ellen, amelyek a napból származnak.

Nem vagyunk rá felkészülve, mert ezen (akkor még ismeretlen) problémák nem képezték a beruházási igény és a tervezési program részét és nem ismertük az ezen beruházások megvalósulásával kapcsolatos utólagos érték változásokat, az informatikai rendszerek felértékelődését.

Az űridőjárás és ebben kiemelten a naptevékenység földi hatásának vizsgálatát mind a **NASA**[106] mind az **ESA**[107] kiemelte kezeli, mert ezzel egy új kockázati elem merült fel, amire érdemi választ kell adni.

A felmerülhető veszélyek kapcsán, csak a leglényegesebb okozatok figyelembevételével folytatnám gondolatmenetemet, nem a naptevékenységről kívánok értekezni, hanem annak hatásait értékelendő javaslatok összeállítását tűzetem célul.

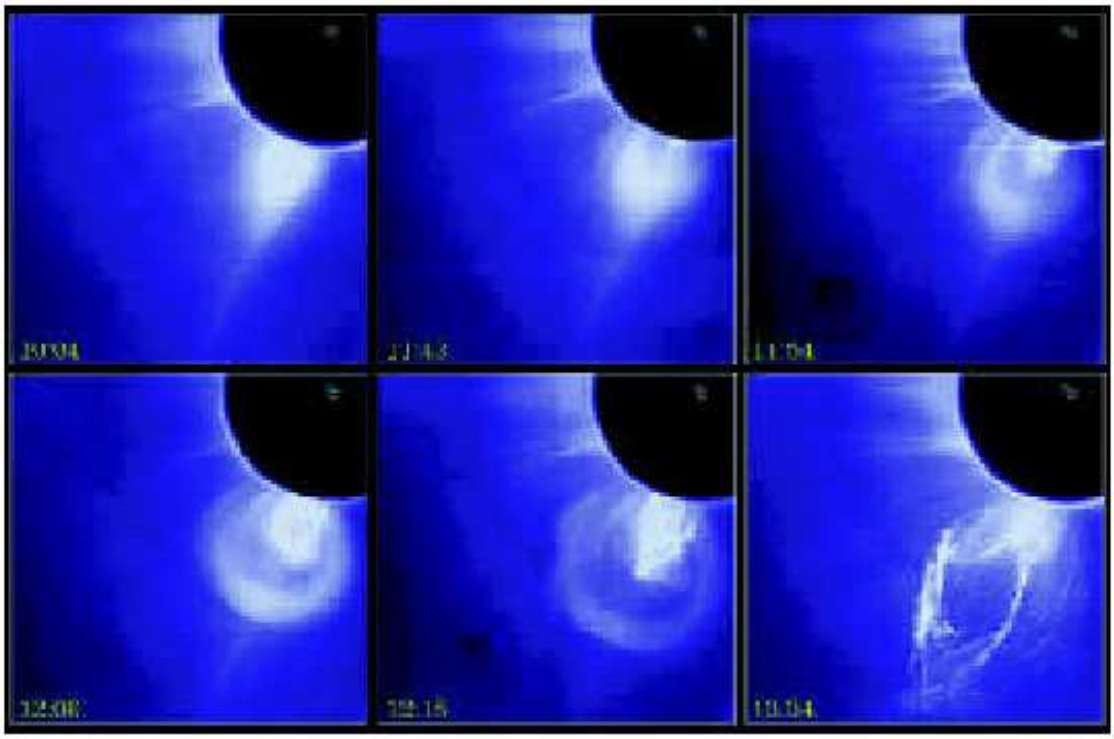
A NASA **SOHO**[108] programja, a **So**lar and **H**eliospheric **O**bservatory a naptevékenység földi hatásaival és a naptevékenység megfigyelésével, előrejelzésével foglalkozik.

A **nap tevékenységének**[109] olyan elemeit figyelik és kutatják, amelyeknek közvetlen kihatása lehet a földi életre és a földi- földkörüli kritikus infrastruktúrákra.

[106] NASA (National Astronautic and Space Administration):http://sohowww.nascom.nasa.gov/spaceweather/
[107] ESA (European Space Agency) honlapról: http://www.esa.int/esaMI/SSA/SEM0MNIK97G_0.html
[108] SOHO: http://sohowww.nascom.nasa.gov/spaceweather/
[109] Visszamenőleges nap adatok: http://www.lmsal.com/solarsoft/latest_events_archive.html 2002-ig.

CME – Flare – Napkitörés.
Ezen nap hatásokból, angolból saját fordításomban a Kritikus Infrastruktúrára legveszélyesebbet ismertetem [110]:

Bubble – **C**oronal **M**ass **E**jection (**flare**)
CME = **Flare** = Felfúvódás, Korona kilövelés



The bubble of plasma in a CME expands and grows more potent until it escapes from the magnetic and gravitational energy of the Sun.

A napkitörés (CME) plazmagömbje, amely addig expandál és növekszik, amíg meg nem szökik a nap mágneses és gravitációs energiateréből.

Egy a napot elhagyni képes CME, a napot egy örvényhullámként hagyja el és átlagos sebessége eléri a 400 Km/másodpercet. (Egy-két nap alatt éri el a földet.) Ahogy a kilökődött CME a folyamatos napszéllel egyesül, abban egy lökés hullámot hoz létre, amely átrepül a naprendszeren és bolygókat, aszteroidákat és egyéb égi objektumokat bombáz.

[110] Forrás: NASA honlap: http://www-istp.gsfc.nasa.gov/istp/outreach/cmeposter/index.html

Ha a CME a napnak a föld felé néző felén tör ki és bolygónk keresztezi ennek a kiáramló anyagfelhőnek az áramát, úgy ennek az eredménye igen látványos, de néha veszélyes is lehet.

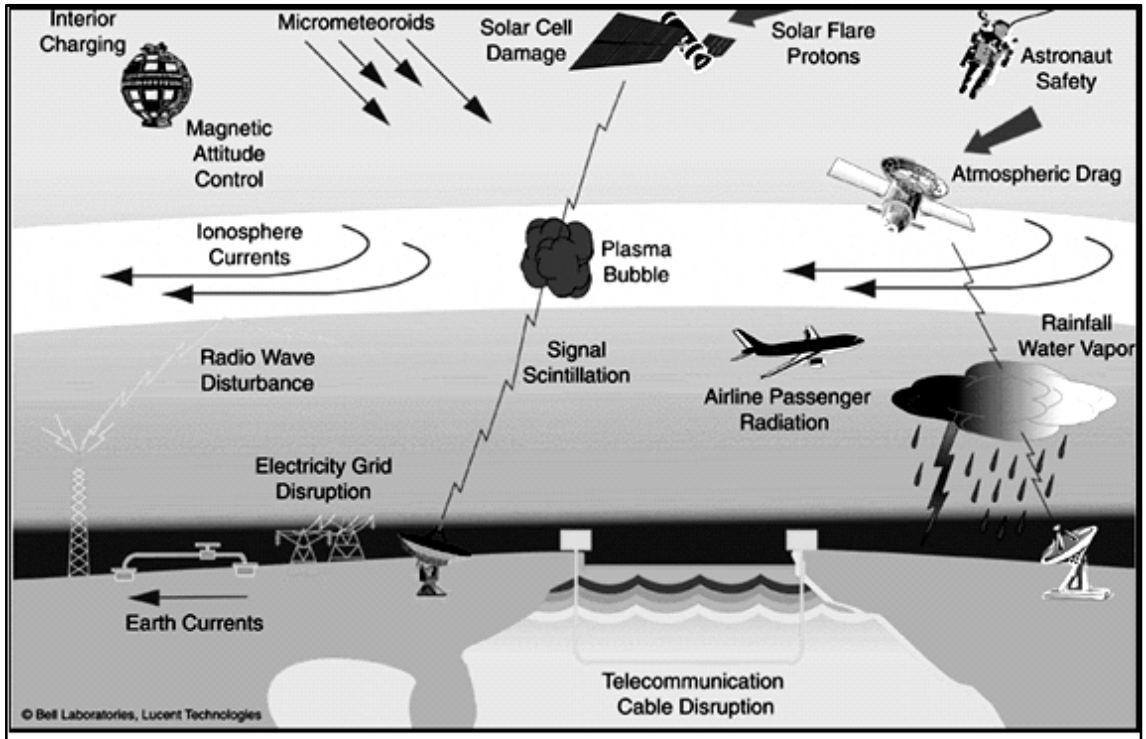
A legismertebb CME hatás, az elsősorban a föld északi és déli pólusán megfigyelhető, Alaszkában az (Európában Svédország és az északi államok) északi fény (aurora) jelensége, amely a naptevékenység erejétől függően megjelenhet akár Texas (Európában a déli államok) magasságában is.

Seen here over Alaska, auroras are native to the far northern and southern lands. The most powerful magnetic storms can bring auroras all the way to Texas.

Ezek a plazma által gerjesztett mágneses viharokés jelenségek esősorban a magnetoszférára korlátozódnak. Az űrből származó plazma a magnetoszférának üközve a Van Hallen övezet elektronjait, protonjait és oxigén ionjait gerjeszti ez által az övezet ion sugárzása gerjesztetté válik: sűrűbb, forróbb és gyorsabb lesz. Ha ezek a gerjesztett magnetoszféra áramlások elérik a felső légkört és az ott lévő oxigén és nitrogén molekulákkal ütköznek, úgy emissziós (fluoreszkáló) fény keletkezik. Ezt látjuk a földről az északi-déli[111] fényjelenségnek.

[111] FOTO: Forrás: NASA honlap: http://www-istp.gsfc.nasa.gov/istp/outreach/cmeposter/index.html

A CME sugárzások jelentős részét azonban szabad szemmel nem érzékeljük. A CME áramlás egyaránt tartalmaz szabad szemmel látható elektromágneses hullámokat (fény), de tartalmaz röntgen és gamma sugarakat, valamint ultraibolya sugárzási tartományokat is.
A föld és az űrből érkező sugárzások vizsgálatára indult az **I**nternational **T**errestrial **P**hysics (**ISTP**) program, amely 25 satelitből álló flottájával vizsgálja ezeket a jelenségeket.
A mérések azt mutatták, hogy egy átlagos, a földet elérő CME 1500 Gigawatt elektromos energiával üti meg a magnetoszférát.(Ez az USA energiatermelésének a kétszerese) ami hatalmas változásokat képes okozni az űrben és akár a földön is.



The effects of magnetic storms - what scientists call space weather - extend from the ground to geostationary orbit and beyond.

A fenti rajz [112] összefoglalja a lehetséges károkat:
Solar flare protons: CME protonáramlása, tönkreteheti a műholdak napenergia celláit és veszélyezteti az űrhajósok egészségét.
Az ionoszférát elérve és ott plazma gömböket létrehozva zavarással akadályozza a földi állámások kapcsolatát az űrbéli eszközökkel, ezzel akadályozza a repülőgépek (GPS) irányítási rendszereit és az utasokat

[112] Forrás:NASA SOHO: http://www-istp.gsfc.nasa.gov/istp/outreach/cmeposter/blackout.html

sugárveszélynek teszi ki. Zavarja a földfelszíni rádióadásokat. Zavarokat okoz az elektromos ellátásban és gerjesztett áramot indukál a hosszú távú kőolaj vezetékekben és kommunikációs hibákat okoz a tengeralatti kommunikációs kábelekben.

Ezeket a veszélyeket az elmúlt évtizedekben sajnos már az emberiség megismerte [113] a következő részt szó szerint idézem:

Korábbi évtizedekben bekövetkezett káros események:

„ A flerek (CME) az ibolyántúli részen többszörös, a röntgentartományban pedig már több nagyságrendnyi sugárzásnövekedést okoznak. Erre az ionoszféra érzékenyen reagál. A röntgensugárzás hatására megnő a D-réteg ionizációja, ami erőteljes elnyeléshez vezet a rövidhullámok tartományában (fading). Ugyanakkor a megnövekedett ionizáció miatt az ionoszféra olyan ultrarövid hullámokat is visszaver, amelyeket egyébként átengedne. Hasonló következmény, hogy a közepes szélességeken megnövekszik a nagyon nagy (kb.10 km) hullámhosszúságú légköri rádiózaj erőssége. Ezt a zajt az állandó trópusi zivatarok villámai keltik, s az ionoszféra D-rétegéről visszaverődve jutnak el hozzánk. A fenti zavarokat a flerek elektromágneses sugárzása okozza, amely minden, a Nap felénk forduló félgömbjén látható flerekből elér a Földre, és a fénysugárzással egyidejűleg érkezik.

Megfigyelték, hogy már kis geomágneses aktivitás hatására elektromos áram indukálódik a vezetékben.

Az ilyen jellegű megfigyelések már a múlt században kezdődtek, mikor kiépültek a telegráfvezetékek.

1859-ben megfigyelték, hogy sarki fény idején, azaz mágneses viharban hiába kapcsolták le a hálózatot a feszültségforrásról, a hálózat a lekapcsolásra fittyet hányva működik tovább. Fölfigyeltek arra is, hogy a vezetékben indukált áram ingadozásai összefüggésben állnak a sarki fény intenzitásának ingadozásával.

A nagyobb napkitörések által kiváltott geomágneses viharok néha egészen megdöbbentő hatásokat hoznak létre ezekben a vezetékekben.

[113] Forrás: Idézet SZTE, Klein Tamás matematika fizika szakos hallgató szakdolgozat, 2000. Címe: „A nap és a naptevékenység földi hatásai” Témavezető: Dr. Szatmáry Károly tudományos főmunkatárs.

Az **1978. január 10-11**. között lejátszódó geomágneses vihar például az USA-t Skóciával összekötő Transzatlanti vezetékben 2700 V-os feszültséget indukált. Ennek hatására több városban szinte teljesen összeomlott a telekommunikációs hálózat.

Észak-Amerikában szintén jó példákat találunk az erős geomágneses viharok hatására, a magas feszültségű hálózatok furcsa viselkedésére.

1958-ban Torontóban geomágneses vihar következtében megsemmisült az áramelosztó rendszer, aminek hosszabb áramkimaradás lett a következménye. Hasonló eset történt:

1972 szeptemberében az USA-ban, amikor a nagy napaktivitás hatására a túlterhelődött transzformátorok felmondták a szolgálatot.

1989-ben volt a legutolsó nagy geomágneses aktivitás melynek hatására némely kanadai telefonhálózat vezetékében 80-150 A erősségű indukált áramot mértek.

A gáz- és kőolajvezetékekre is jelentős hatással van egy nagyobb napkitörés, geomágneses háborgás. Ezeket a vezetékeket úgy védik a korrózió ellen, hogy a vezetéken áramot vezetnek keresztül. A védőáramot szolgáltató és ellenőrző berendezések a geomágneses háborgások alatt túlterhelésnek lehetnek kitéve. Jó példa erre az Alaszkában található, 1300 km-es kőolajvezeték, amelyben:

1978. augusztus 5-én 85A nagyságú indukált áramot és 130000 V/km nagyságú térerősséget regisztráltak.

A naptevékenység hatással van a földi időjárásra is (lásd Maunder-minimum). Több esetben sikerült kimutatni időjárási elemek, (mint például a csapadékmennyiség vagy a hőmérséklet) 11, ill. 22 éves periodikus változását. Ilyen pl. az USA délkeleti és Mexikó északi része között elterülő sivatag területe, amely kb. 22 éves időközönként felváltva nő és csökken, ami ciklikus aszályokat okoz a Mississippi folyótól nyugatra eső vidékeken.**”**

A fenti megalapozás szerint, a legveszélyesebb naptevékenység észlelése és annak földi kihatása között 12-24 óra időkülönbség van. Tehát van idő a reakcióra.

Lehetőség van a leginkább veszélyeztetett rendszerek üzemszerű leállítására és a legfontosabb átmeneti intézkedések megtételére.

Nos, ennyi veszélyismertető után nézzük, milyen tanácsaink is lehetnek gyakorlati szinten az IT szakemberek számára?

TARTÓS HÁLÓZAT KIMARADÁS PROGNÓZIS ESETÉN:

Megtehető intézkedések:

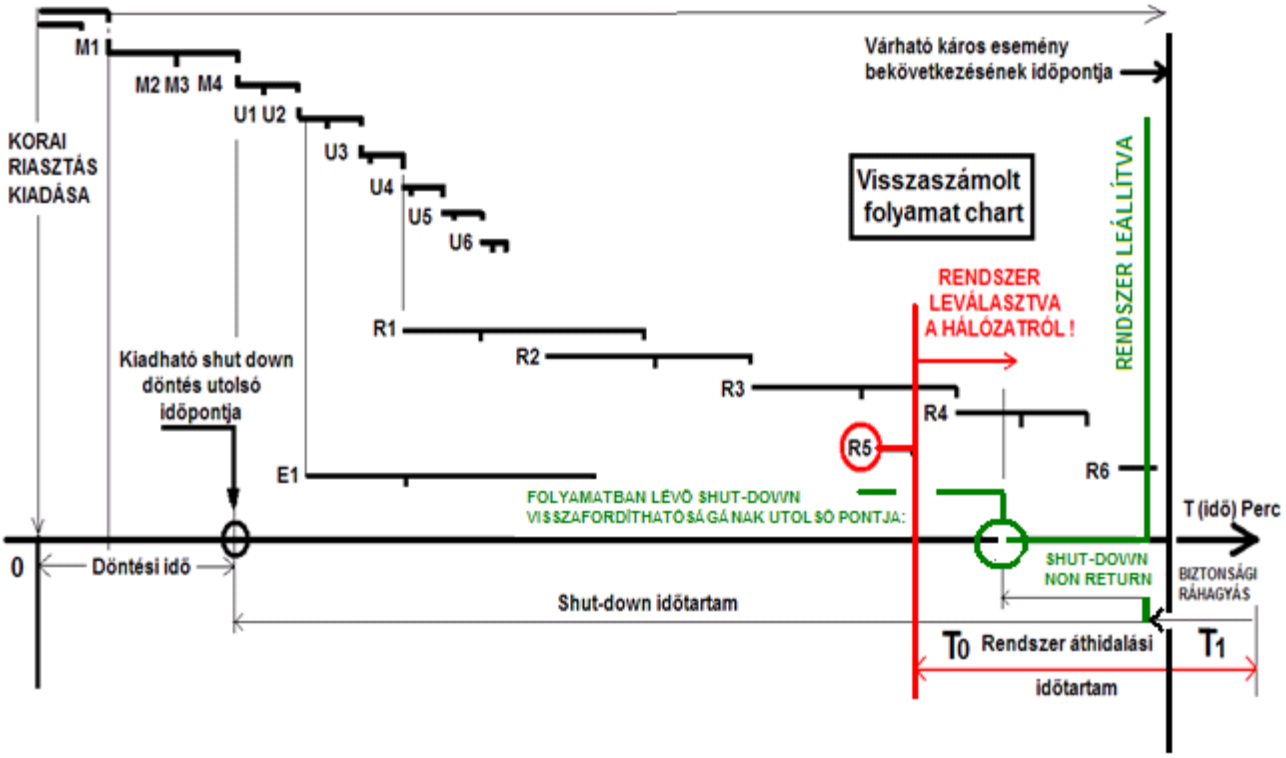
1/ RENDSZER SHUT-DOWN ÉS ALÁBBI MEGFONTOLÁSAI:

Figyelem az alábbi táblázat[114] egy nagyobb vállalatra vonatkozó fiktív időket tartalmaz, tehát csak jelezni kívánom a probléma összetettségét.
A shut-down időt a várható előre jelzett várható káros esemény bekövetkezte előtti időpontból (biztonsági ráhagyással) visszafele számolva kell kialakítani.
Javaslatom szerint: ezt az ISMS-ben szabályozható módon, egyediesítve kell felmérni és bevezetni.

SORSZÁM	RIASZTÁS:	FELADAT	ÁTFUTÁSI IDŐ (PERC)
M1	Első szint:	MENDZSMENT értesítése és döntés	60-120
M2		RENDSZERGAZDÁK értesítése	30-60
M3	Második szint:	USER-ek értesítése	30-60
M4	Harmadik szint:	EGYÉB MUNKAVÁLLALÓK értesítése	30-60
	USER Feladat:		
U1		Aktuális munkák lezárása, elmentése	10-50
U2		Adatbázis USER kapcsolatok megszüntetése (kilépés)	10-30
U3		KLIENS kilépés a hálózatból	5-10
U4		Gép kikapcsolás	3-10
U5		Áramkapcsolat fizikai megszüntetése	2-5
U6		Hálózati kapcsolat fizikai megszüntetése	2-5
	RENDSZERGAZDA Feladat:	HÁLÓZAT MÉRETÉTŐL FÜGGŐEN	
R1		Aktuális munkák lezárása, elmentése	60-300
R2		USER kilépések ellenőrzése, manuális kiléptetés	100-200
R3		KLIENS hálózati kilépésének ellenőrzése, kiléptetés	100-200
R4		Adatbázisok és szerverrek shut-down	30-120
R5		Szerver áram kapcsolat fizikai megszüntetése	5-10
R6		Hálózati kapcsolat fizikai megszüntetése	5-10
E1	EGYÉB MUNKAVÁLALÓK Feladat:	Áramtalanítás áram kapcsolat fizikai megszüntetése	30-120

[114] Forrás: A Szerző által saját tapasztalatai alapján összeállított elvi táblázat.

A következő általam[115] készített Gant – diagram, azt mutatja, milyen lehetőségeink lehetnek egy előzetes korai riasztás esetén a döntések meghozatalára. **A rendszer károsodás megóvására olyan esetben, amikor a teljes IT rendszert az elektromos hálózat felől várható áramlökés miatt előbb fizikailag lekapcsoljuk a hálózatról, és a shut-down hátralévő részt, a kellő biztonsággal ráhagyott UPS vagy más tartalék energia felhasználásával folytatjuk le.**



2/ KÖLTSÉGFEDEZET ELEMZÉS:

Meglévő rendszereink üzemeltetése és veszélymegelőzése kapcsán tisztázni kell, hogy melyik érték modell illetve melyik költség függvény alkalmazandó. (Lásd: Döntési modellek fejezet, 24. és 27. oldal)

[115] Forrás: A Szerző által saját tapasztalatai alapján összeállított elvi ábra.

3/ OPERATIÍV INTÉZKEDÉSEK:

Ennek függvényében a ráfordítási lehetőségek (korlát) ismeretében kell megtenni intézkedéseket:

- UPS és tartalékáram (aggregátor) rendszerek megelőző felülvizsgálata[116] (Lásd: Jelen tanulmány: 64.-66. oldalakon)
- Kitartási idő felülvizsgálata és az ellátott rendszerek terhelés igényének egyeztetése különös tekintettel az IT és kiszolgáló hűtés rendszerre.
- Hálózati rendszer betáplálási pontról való fizikai lekapcsolás lehetőségének megvalósítása
- ESA riasztási rendszer és annak figyelemmel kísérése
- A rendszer teljes shut down idejének felmérése (Lásd:81.-82.oldal.)
- ISMS definiálása a vészhelyzetre.

4/ ISMS (VAGY MÁS FELKÉSZÜLÉSI TERV):

szerinti képzés és működés, az ISMS- re figyelemmel való beruházás előkészítés. (Lásd: Jelen tanulmány 34-35. oldalon tett javaslatok.)

5/ EGYÉB MEGTEHETŐ ALTERNATÍV INTÉZKEDÉSEK:

Itt elsősorban, olyan lehetőségek kidolgozását és szervezési eszközök tartalékként rendelkezésre állítását érték, amelyekkel teljes leállás esetén is a munka egy bizonyos ideig még rendszer nélkül is folytatható. (Lásd: Jelen tanulmány 59., 62.-63. oldalán leírt intézkedések)

6/ ADATÁLLOMÁNY MENTÉSEK

Redundáns mentési rendszer. Adatállományok (ahol az adatállományok mérete, ezt megengedi) mentését szilárd adathordozóra is célszerű megtenni. Pl.: CD, DVD, BLUE-RAY (kisebb elektromos kockázat).

ISMS szerint a nem információ érzékeny munkahelyeken elvárható, hogy a munkavállalók saját munkájuk mentéseit CD, DVD-n folyamatosan maguk is végezzék.(Ne hagyatkozzanak kizárólag a központi mentésekre.) Ezt a megoldást, egyes ISMS, kifejezetten vállalati (üzleti) információkat védő vonatkozásai természetesen felülírhatják.

[116] Közelmúltban egy általam megismert banki projekt kapcsán, IT igények indokolták az UPS és aggregátorok, valamint a számítógép terem klíma bővítését és egységes ellátási (fenntartási idő) kialakítását. 2N+1 moduláris UPS, +1 aggregátor telepítését és a klíma redundanciák felülvizsgálatát.

7/ Új beruházások előkészítő fázisában, már a beruházói igény összefoglalást biztonsági fokozat szemléletben (TIER) és megelőzési költségelemzésnek alávetve célszerű lefolytatni.(Lásd: Jelen tanulmány 67-től 74. oldalig)

Felhasznált irodalom:

Frank András, ELTE TTK. 2011 Operációkutatás egyetemi jegyzet

Andrew S. Tannenbaum, Prentince Hall –Computer Networks. 3. edition. 1999 PANEM

Novosel-Hudson-Stewart TCP/IP 2000. Kiskapu kiadó

Reynders-Wrigth TCP/IP és ETHERNET hálózatok a gyakorlatban 2005. Kiskapu kiadó

A Szerzőnek a Legfőbb Ügyészség egyik pályázatán, a Legfőbb Ügyész különdíját nyert pályaműve.

Miskolci Egyetem, Vállalkozáselmélet- és Gyakorlat, Doktori Iskola, Várkonyiné Juhász Mária 2008 PhD. értekezés. Címe: „Az érék fogalmának változásai és könyvvizsgálatának kérdései a hazai szabályozás tükrében."

Magyar Sportenciklopédia A-K 2002. Kossuth kiadó

Glevitzky Béla, Operáció kutatás 1. mobiDIÁK könyvtár sorozat, 2003. Kiadó: Debreceni Egyetem

Information Technology Capability Maturity Framework, 2009. Prof. Dr. Martin Curley

Kornai János: A hiány. 1980,1982,1989 Közgazdasági és Jogi Kiadó

TOGAF The Open Group Architecture Framework 2009. kiadás

Dr. Nádori László: Edzéselmélet és módszertan, 1984. Testnevelési Főiskola tankönyv

IVSZ: Informatikai Vállalkozások Szövetsége ajánlása, 2010, Iparági egységes fogalomtár v11

TIA 942 szabvány

ISO 27000:2006 ISMS

ITIL: Information Technology Infrastructure Library

1959. IV tv. A Polgári Törvénykönyv Magyarázata, 1992. Közgazdasági és Jogi Kiadó

Eörsi-Kemenes-Sárány-Világhy: „Kötelmi Jog (különös rész)" 2002.Nemzeti Tankönyvkiadó

MS-DOS 6.1 User Guide 1994, MICROSOFT Corporation

MS Windows for Workgroups 3.11 1990, MICROSOFT Corporation

Kernighan & Pike: „A UNIX operációs rendszer" magyarul 1987, Műszaki Könyvkiadó

Borges & Eisler: „PC-hálózat építés" magyarul, 1997 PANEM kiadó

Szlovák-Tóth- Kőri: „Adatbázis kezelés, programozás dBASE IV-ben" 1989, LSI

Klaus Dembowski, „PC táblázatok" 1997, Kossuth kiadó

Göncöl-Korinek-Lévai:„Kriminológiai ismeretek, bűnözés, bűnözés kontroll" 1999 CORVINA

Kevin LONEY, ORACLE DATABASE 10g – Teljes referencia kézikönyv, 2006 PANEM kiadó

SZTE, Klein Tamás matematika fizika szakos hallgató szakdolgozat, 2000. Címe: „A nap és a naptevékenység földi hatásai"

Hivatkozott szabványok: ISO/EEC 27000:2006 (ISMS), TIA 942, ITIL v3,
Hivatkozott módszertanok: PRINCE2, TOGAF,