EGYMÁSRA, EGYMÁSBA ÉPÜLŐ IRÁNYÍTÁSTECHNIKAI RENDSZEREK KRITIKUS PONTJAI

2016.02.17.

Az Energetikai Szakkollégium 2016. tavaszi félévének első, az Egymásra, egymásba épülő irányítástechnikai rendszerek kritikus pontjait bemutató előadása, február 17-én került megrendezésre, a Magyar Elektrotechnikai Egyesület Energetikai Informatika Szakosztályával közösen. A rendezvényt az Evopro Kft. képviseletében Sinka Lajos Úr tartotta a Budapesti Műszaki és Gazdaságtudományi Egyetemen. Előadása során az érdeklődők részletesen hallhattak az irányítástechnikai rendszerek kialakítása során figyelembe veendő evidenciákról, így például a bemenő információ megbízható áramoltatásáról, a redundancia szükségességéréről és fontosságáráról fejlesztői szempontból, a redundancia és az információk degradációjából eredő kérdésekről, az információk megbízhatóságáról és rendelkezésre állásáról, valamint a kialakult degradált üzemállapotok kezeléséről.

BEVEZETÉS

Sinka Lajos Úr az előadás elején a fontosabb fogalmak bemutatására helyezte a hangsúlyt. Ennek keretében megtudhattuk, hogy a leíró modellünk céljától nagymértékben függ, hogy mit is tekintünk információnak. Az információ valójában a körülöttünk tapasztalható mintázatról szóló, és az arról, általunk kialakított, „vetített", közvetített kép maga.

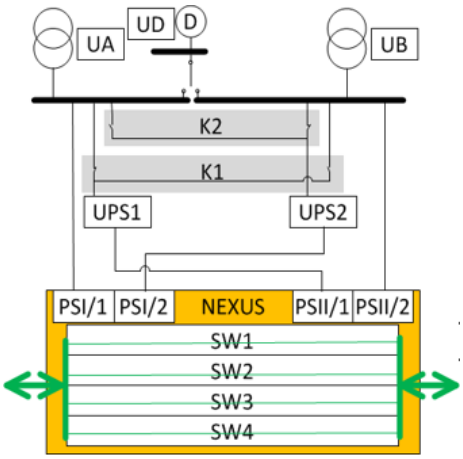
TERVEZETTSÉG

Rendszereink létrehozása során elengedhetetlen fontossággal bír, hogy minden szinten tervezzünk, különös figyelmet fordítva a meghibásodásokra, degradációkra. Alaprendszerünknél szükségszerű, hogy az az „n-1" szabályt teljesítse („n" állapotú rendszerünk egy hibát tűr, és jelez). Ennek az állításnak az értelmét, lényegét, a tervezett rendszereink lényegévé kell tenni.

Összetett rendszereken belül, a folyamatos leépülés különböző szintjeit meg kell terveznünk. Az ezekbe történő belépésről tudnunk kell, információt kell róla szolgáltatni. A végsőcél, hogy a degradált állapotból minél hamarabb vissza tudjunk jutni a teljes rendelkezésre állás állapotába (amit a teljes, tervezett tartalékoltságnak tekintünk), úgy, hogy a 100 %-os működőképességet a degradált állapotban is megőrizzük.

Az irányítástechnikai rendszereink nem öncélúak, üzemviteli célokat szolgálnak. Erről sok esetben megfeledkezünk. Napjainkban az üzemviteli területek mellett az irányítástechnikai rendszerek is egyre összetettebbé, komplexebbé váltak, elkezdtek redundanciákra épülni. Ma már nem az jelenti a legnagyobb gondot, ha hiba lép fel, hanem az, ha a hibát nem vesszük észre, nem jelezzük, és adott keretidőn belül

nem tudjuk elhárítani. Ennek eredményeképpen a rendszereink tervezésének fókuszában ezeknek a céloknak is ott kell szerepelniük.

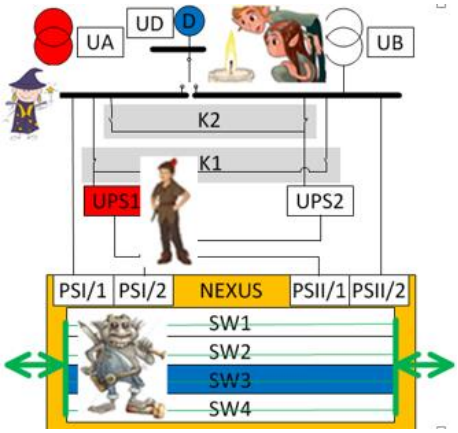


ADATKAPCSOLATI ELEM TERVEZÉSE

Előadónk egy érdekes példán keresztül mutatta be egy adatkapcsolati rendszer működését, meghibásodását.

Célunk, egy nagy értékű, folyamatos gyártósori termelés biztosítása. Ehhez olyan eszközöket kell alkalmaznunk, melyek menedzselhetőek, illetve nagy megbízhatóságú adatkapcsolattal, és kiterjeszthető rendelkezésre állási idővel bírnak.

A tervezési korlátnak tekinthetjük – a hibajavítás szempontjából – hogy alapvetően a folyamatos üzemvitelt kell biztosítanunk, és hiba esetén biztosítanunk kell a kockázatmentes leállításhoz szükséges időt. Mind adatkapcsolati, mind megtáplálási szinten intelligens, menedzselhető redundanciát kell biztosítanunk. Megfelelő üzemeltetési feltételeket létrehozva, mindegyik egységünk folyamatosan teszi a dolgát.



Ha egyszer csak Rontó Pali megérkezik, és ütemezett karbantartást szeretne végrehajtani az SW3 switch-csen, lehetséges, hogy véletlenül mellé nyúl. Figyelmetlenségének köszönhetően az UPS1 megadja magát, és egy rendszerszintű hibajelzés generálódik. A menedzselhetőség miatt az n-1-es redundancia egy hibát tűr és ugyanennyit jelezni is képes, így értesülhetünk az okozott kellemetlenségekről. Ezt követően Szerviz Jani korrigálja az UPS hibát, de a technológia által erősen korlátozott ideje van csak a javításra. Ekkor Huncut Démon az UA betáplálás transzformátorát túlmelegíti és kiejti. Ezáltal kritikus üzemállapot jön létre rendszerünkben. Minderről az üzemeltetők a hibajelzésekből értesülnek. Pöccentős Juci és Töltős Marci kivonul a diesel berendezéshez, és figyelik az életjeleket. Ha szükségét érzik, akkor pöccentenek egyet a diesel egységen. Az Ő tevékenységüket viszont már nagyon sok menedzser figyeli és irányítja.

A kialakult helyzetben a menedzser kétféleképpen dönthet:

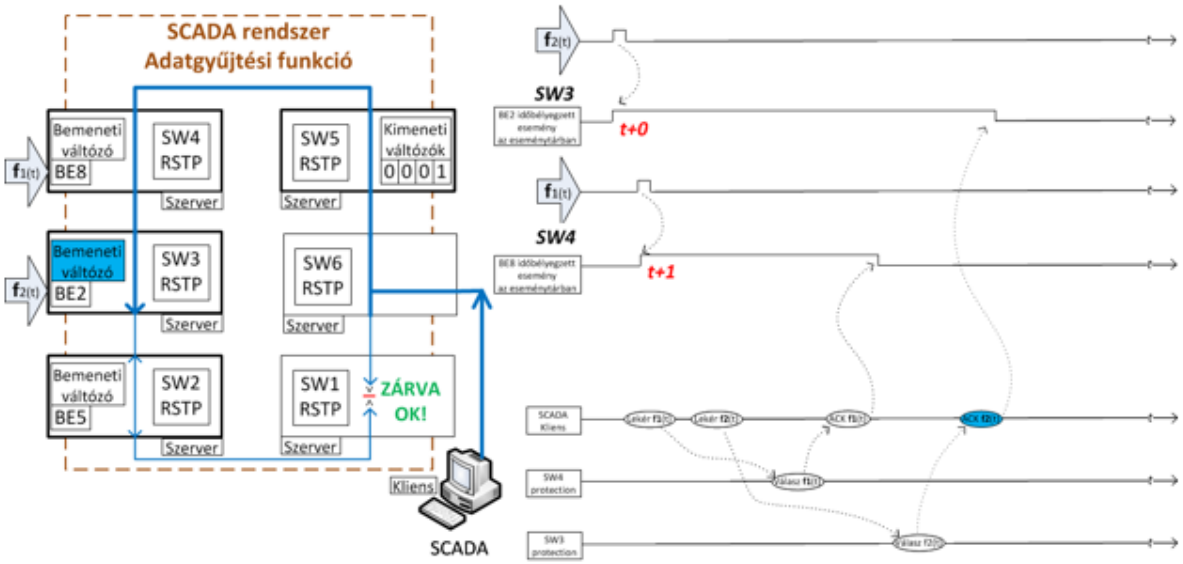
1. eset: Megállítja a gyártást, és kockáztatja, hogy garantált termelés kiesés történik. Ebben az esetben viszont nem keletkezik a gyártósoron elromlott termék, és lehet,

hogy a kritikus állapotot is sikerül felszámolni a rendelkezésre álló tartalékok segítségével.

2. eset: Nem állítja meg a gyártást és így nem történik garantált termelés kiesés. Ellenben keletkezhet a gyártósoron elromlott termék, és lehet, hogy a kritikus állapotot nem sikerül felszámolni a rendelkezésre álló tartalékok segítségével sem.

ÖSSZETETTEBB SCADA RENDSZER MŰKÖDÉSE ZAVARÓ TÉNYEZŐ NÉLKÜL

Előadónk, egy, három független alkalmazást, alrendszert, tartalmazó rendszert hozott példaként, hogy bemutassa egy komplexebb egység működését. A rendszeren belül egyedi védelmi készülékek helyezkednek el switch-csel kiegészítve. A hálózatba kapcsolt terepi készülékekből a SCADA rendszer gyűjt adatokat, négy darab terepi készülék pedig a kommunikációs rendszeren keresztül integrált automatika funkciót valósít meg. Az így kialakított egyszeres hurok csak az átviteli közeg hibát tűri el (a rendszer n-0,5 hibát tűr, és jelez). Aki ilyen rendszert épít, annak figyelembe kell vennie, hogy hibatűrés szempontjából teljesen feleslegesen dolgozik.



1. ábra SCADA rendszer működése zavaró tényező nélkül

Elsőként zavaró tényező nélkül vizsgáltuk meg a rendszer működését. Kezdetben a BE2 bemeneten érkezett változás, melyet egy impulzussal jelöltünk (1. ábra). Az impulzus két eseményt jelent, példánkban viszont csak az első változás hatását, a felfutó éllel reprezentált változást értékeljük ki. Amint megérkezett a változás érzékeltük, azonosítottuk, időbélyeget adtunk neki, és eltároltuk az eseménytárban. Ezután a BE8 bemeneten érkezett egy másik változás, mely hasonlóan az előzőhöz, az eseménytárba íródott. A SCADA rendszer megvizsgálta, hogy van-e esemény a terepi készülékek eseménytárában.

A SCADA rendszer észlelte, hogy változás történt az eseménytárakban, ezért kezdeményezte az $f_1(t)$ t+1 esemény felolvasását. Ezzel „párhuzamosan" az RSTP MASTER indirekt módon ellenőrizi a hálózat működését. A logikailag nyitott hálózaton az ellenoldalra is megérkezett a távirat (ECHO). Ezután a SCADA rendszer kezdeményezte az $f_2(t)$ t+0 esemény felolvasását is. Közben az RSTP a háttérben folyamatosan dolgozott. Az SW4 készülék elküldte az $f_1(t)$ t+1 eseményt leíró táviratát. A SCADA nyugtázta a távirat vételét, és az SW4 törölte az $f_1(t)$ t+1 eseményt az eseménytárjából. Ezt követően az SW3 készülék is elküldte az $f_2(t)$ t+0 eseményt leíró táviratát, melynek vételét a SCADA szintén nyugtázta. Végül pedig az SW3 is törölte az $f_2(t)$ t+0 eseményt az eseménytárjából.

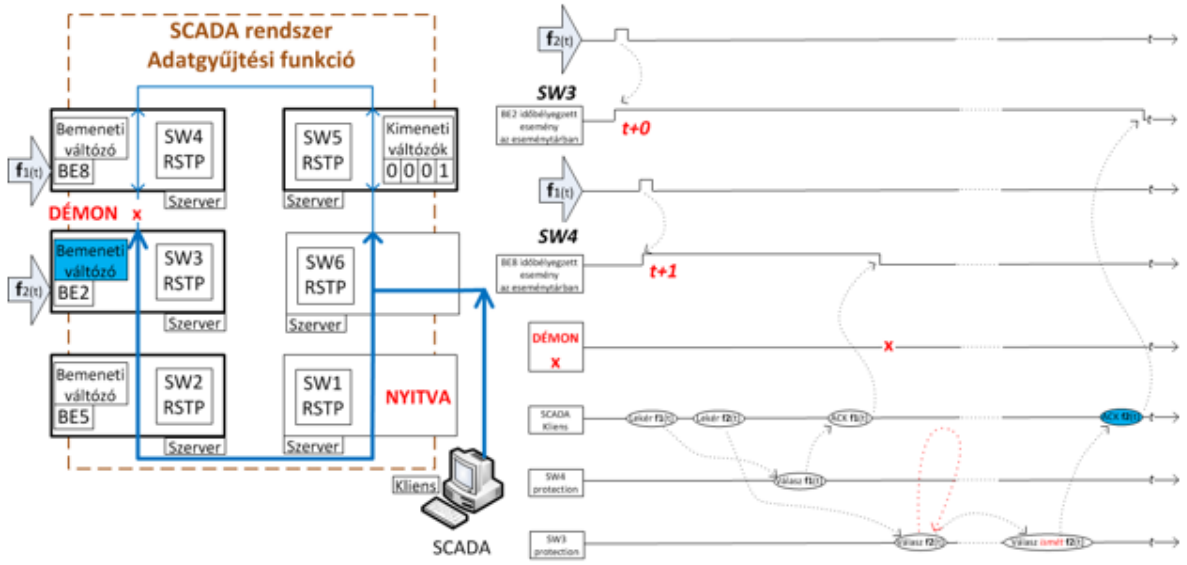
A vázolt példa során megfigyelhettük, hogy az $f_2(t)$ t+0 változás, az $f_1(t)$ t+1 változásnál, korábban bekövetkezett, annak ellenére, hogy később szereztünk róla tudomást. A SCADA rendszerünk az eseménynaplójában a változásokat az időbélyegük alapján időrendi sorrendben publikálja. Az időrendi sorrendezés folyamatában a SCADA figyelembe veszi a saját lekérdezési ciklusainak időintervallum hosszát.

Összességében tehát elmondhatjuk, hogy az adott felbontással az alrendszerünk hibátlanul működött.

Összetettebb SCADA rendszer működése zavaró tényezővel

A következő példa során megfigyelhettük, hogy milyen hatással van rendszerünkre egy zavaró tényező. Tételezzük fel, hogy a BE2 és a BE8 bemenetekre megérkeznek a változások. A SCADA megvizsgálja, hogy van-e esemény az eseménytárban. Ekkor észleli, hogy van, és kezdeményezi az $f_1(t)$ t+1, majd az $f_2(t)$ t+0 esemény felolvasását. Az SW4 készülék ezután elküldi az $f_1(t)$ t+1 eseményt leíró táviratát, melynek vételét a SCADA nyugtázza. Ezt követően az SW4 törli az $f_1(t)$ t+1 eseményt az eseménytárjából. Ekkor viszont jön egy DÉMON, mely megrongálja - az ábrán „x"-el jelölt helyen, és időpillanatban - az átviteli közeget. Az SW3 készülék elküldi az $f_2(t)$ t+0 eseményt leíró táviratát, mely most nem ér célba. Az RSTP észleli a hibát, és gyorsan meg is jegyzi, hogy mi volt az üzenet. Az SW1-ben az RSTP MASTER megismétli a táviratot. Nem sok idő elteltével a SCADA megkapja a táviratot és nyugtázza annak vételét. Kis kavarodás után pedig rendet tesz a sorrendekben.

Megfigyelhettük, hogy az $f_2(t)$ t+0 változás az $f_1(t)$ t+1 változásnál korábban bekövetkezett esemény, de sokkal később érkezik meg a hír róla a SCADA-hoz. A SCADA rendszer eseménynaplójában a változásokat az időbélyegük alapján időrendi sorrendben publikálja. Az időrendi sorrendezés folyamatában a SCADA rendszer figyelembe veszi a saját lekérdezési ciklusainak időintervallum hosszát, illetve a hálózati önjavító ciklusok időintervallumainak hosszát is. Az alrendszerünkben keletkezett hibáról az RSTP állapotváltozása jelzett, melyen Szerviz Jani már dolgozhat.



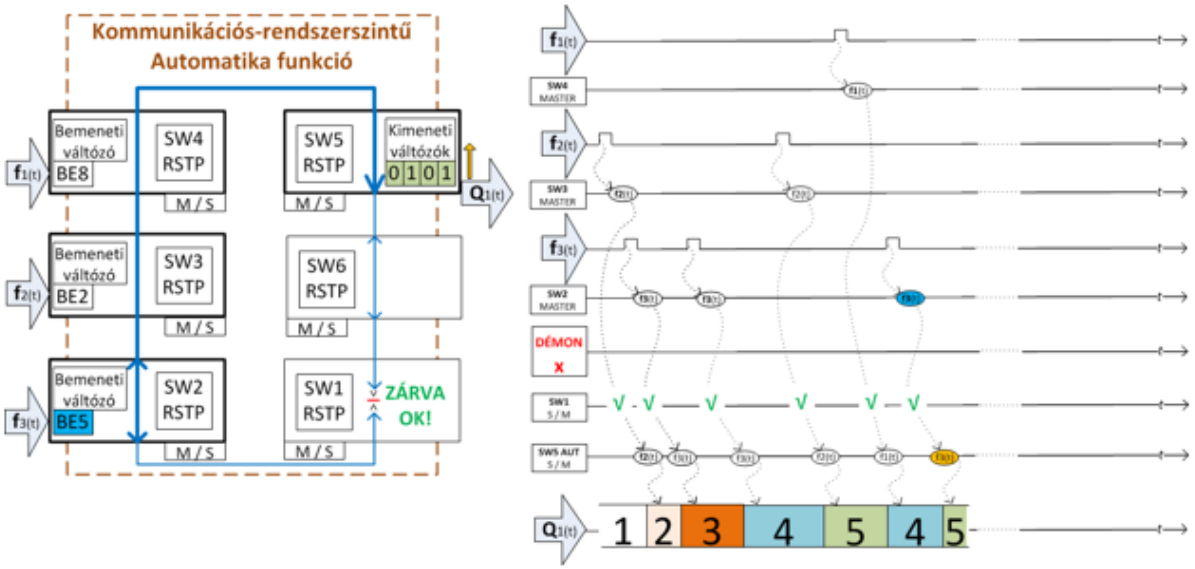
2. ábra SCADA rendszer működése zavaró tényezővel

Védelmek beépített swich-csel, AUT alkalmazása

A fizikai környezet legyen ugyanaz, mint a SCADA esetében, de az SW2, SW3, SW4, SW5 eszközökből alakítsunk ki egy autonóm alrendszert. Az így kapott sorrendi hálózatunk rendelkezik egy hibás állapottal, mely megegyezik az alap, kikapcsolt állapottal, a „0" állapottal. Ezen kívül definiáljunk egy 1-től 5-ig előre, hátra számolót, és tekintsük a számlálói értékeket a rendszer üzemi állapotainak is. Az előadás további részében ezt, a létező rendszerünkön belül létrehozott alrendszert vizsgáltuk, először zavaró tényező nélkül, majd zavaró tényezővel.

Zavaró tényező nélküli AUT

Tételezzük fel, hogy a rendszerünk 1-es állapotban van, mikor a BE2, felfelé számlálást léptető bemeneten, érkezik egy változás, mely hatására az SW3 egy távirat formájában tájékoztatást küld az SW5 készüléknek. Az SW5 megkapja a táviratot, és végrehajtja a tervezői szándékát, azaz eggyel növeli a számláló értékét. Ennek eredményeképpen aktualizálódik a $Q_1(t)$ válaszfüggvény, azaz 1-ről 2-re változik. Ezt követően a BE5, felfelé számlálást léptető bemeneten, érkezik egy felfutó él, és az SW2 egy távirat formájában tájékoztatást küld SW5-nek, aki megkapja a táviratot, és eggyel növeli a számláló értékét. A $Q_1(t)$ válaszfüggvény ezután is aktualizálódik, 3-ra nő az értéke. Ezután ismételten a BE5 bementre érkezik egy felfutó él, és a már ismert folyamatok lejátszódását követően a $Q_1(t)$ értéke 4-re változik. A BE2-re érkező változás a $Q_1(t)$ válaszfüggvényt 5-re növeli, majd a BE8, lefelé számlálást léptető bementre érkező felfutó él hatására a $Q_1(t)$ válaszfüggvény értéke 4-re csökken. A folyamatot a BE5 bemenetre érkező felfutó él zárja, mely 5-re állítja vissza a $Q_1(t)$ értékét. Tekintsük ezt elvárt működési sorrendnek.

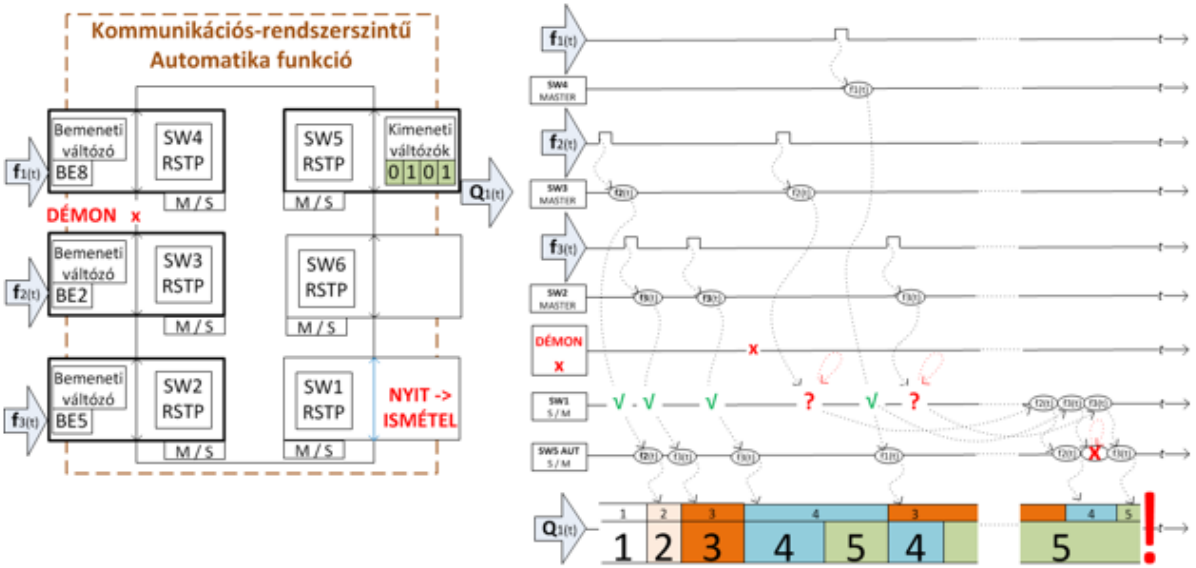


3. ábra AUT rendszer zavaró hatás nélkül

ZAVARÓ HATÁS FIGYELEMBEVÉTELE AUT ESETÉN

A kezdeti állapot (1-es), és a gerjesztő függvény ebben az esetben is ugyanaz. A vizsgálat elején a BE2 bemeneten érkezik egy felfutó él, majd az SW3 egy távirat formájában tájékoztatást küld az SW5 készüléknek. Az SW5 amint megkapja a táviratot, aktualizálja a $Q_1(t)$ válaszfüggvényt, azaz megnöveli eggyel a számláló értékét. Ezt követően a BE5 bemeneten változás történik, az SW2 távirat segítségével tájékoztatást küld SW5-nek, aki amint megkapja azt, végrehajtja tervezői szándékát, és eggyel megnöveli a $Q_1(t)$ értékét. Ez a folyamat még egyszer megismétlődik, így a $Q_1(t)$ értéke már 4-re emelkedik. Ezután érkezik a DÉMON, a zavaró tényező, aki – adott helyen, és adott időpontban - megrongálja az átviteli közeget. Ezt követően, a BE2 bemeneten érkező változásról az SW3 egy távirat formájában tájékoztatást küld az SW5 készüléknek, ami jelen esetben nem ér célba. Az RSTP észleli a hibát, és meg is jegyzi, hogy mi volt az üzenet. Ezt követően a BE8-ra érkezik a felfutó él, melyről az SW4 tájékoztatja az SW5 készüléket. Az SW5 megkapja a táviratot, és teszi a dolgát, de ekkor sincs ECHO, így SW1 ezt a táviratot is megjegyzi. Eggyel csökken az SW5 számláló értéke, aktualizálódik a $Q_1(t)$ válaszfüggvény. A BE5 bemeneten érkező változás hatására az SW2 által elküldött távirat ismételten nem érkezik meg az SW5 készülékhez. Az RSTP ismételten észleli a hibát, és megjegyzi az üzenetet. Ezt követően az SW1 switch-ben, az RSTP megismétli az első táviratot. Az SW5 meg is kapja a táviratot, és végrehajtja a számláló értékének eggyel történő növelését. Ez a folyamat játszódna le újra a második távirattal is, de amint az SW5 megkapja azt, észreveszi, hogy már kapott ilyen táviratot, ezért eldobja azt. Az SW1 switch-ben az RSTP megismétli a harmadik táviratot, mely megérkezik az SW5 készülékhez. Ennek hatására $Q_1(t)$ értéke ismételten eggyel megnő.

A 4. ábráról leolvasható, hogy ugyanarra a gerjesztő függvényre állapotgépünknek sem sorrendiségben, sem pedig állapot idő hosszban nem sikerült ugyanazt a válaszfüggvényt adni.



4. ábra AUT rendszer zavaró hatással

Összességében elmondhatjuk, hogy ilyen módon nem szabad állapotgépet tervezni. A tervezés során, olyan konstrukciót kell kialakítani, amely hasonló, itt bemutatott hibák, események következtében sem adnak más válaszfüggvényt.

Itt vegyük észre, hogy az IT hálózatunk természetes hibatűrő eljárásai vezérelték az állapotgépünket nem elvárt, és így természetes módon nem megengedett állapotokba.

Rendszertervezőként nagyon oda kell figyelni rendszerünk minden apró részletére. Nem csak azt kell tesztelni, aminek a megvalósítása nehezebbnek, összetettebbnek tűnik, az evidenciákra is kellő hangsúlyt kell fektetni. Tesztelésnél mindig a „fekete doboz" megközelítés a célravezető.

A rendszereink helyes működésének elfogadási kritériuma csak az lehet, hogy „azonos gerjesztő függvényre, mindig, minden esetben, „önjavító" hibatűrő eljárások alkalmazása esetén, is azonos válaszfüggvényt kell adni."

Irinyi Dorián
Az Energetikai Szakkollégium tagja