Tarnai Géza: Elektronikus biztosítóberendezések

1. Az elektronikus biztosítóberendezések jellegzetességei [3],[5]

A jelfogós biztosítóberendezések teljes mértékben megfelelnek a biztosítóberendezésekkel szemben támasztott hagyományos elvárásoknak, azonban több olyan hátrányuk van, amelyek a mikroelektronika, illetve az informatika eredményeinek tükrében egyre inkább szembeötlőek. E hátrányok közül elegendő megemlíteni a csaknem kizárólagosan vasút-specifikus elemek (pl. biztonsági jelfogók) alkalmazását, vagy a más, különösen a fölérendelt rendszerekhez való illesztések nagy ráfordításigényét.

A hátrányok kiküszöbölésére kedvező megoldásként kínálkoznak a mikroszámítógépek, a következő tulajdonságaik alapján:

- univerzális alkalmazhatóságuk;
- hardveres és szoftveres strukturálhatóságuk és konfigurálhatóságuk;
- az a lehetőség, hogy az egyes elemekből viszonylag egyszerűen állíthatók össze az igényeknek megfelelő, komplex rendszerek is.

A mikroszámítógépekkel felépített elektronikus biztosítóberendezések alkalmazásának előnyei, többek között:

- a karbantartási ráfordítások csökkentése;
- a munkahelyek ergonómikus kialakítása;
- egységes, a biztosítóberendezés típusától, illetve gyártójától független kezelőfelület alkalmazásának lehetősége;
- az automatizáláshoz és a diszpozícióhoz szükséges kiegészítő funkciók egyszerű integrálása;
- szabványosított illesztőfelületek a mellé- és fölérendelt egyéb rendszerek csatlakoztatásához;
- a rendszer felépítéséből adódóan a szükséges változtatások üzem közben, a berendezés leállítása nélkül előkészíthetők, illetve gyárilag előre levizsgálhatók, és az átállás a programtároló egységek cseréjével egy rövid, vonatmentes időszakban is megoldhatók.

Rendszerstruktúra

A modern üzemvitel számára fontos, hogy lehetőleg minél nagyobb területek üzemi folyamatait egyetlen központból lehessen vezérelni és ellenőrizni. A központ és az egyes onnan irányított berendezések távolsága több tíz vagy akár száz kilométer is lehet. Ebből adódóan a centralizálás szintjének meghatározásánál célszerű az egyes berendezésrészek tulajdonságainak megfelelően, differenciáltan eljárni. Így például a külsőtéri elemeket, mint folyamatperiféríákat vezérlő és ellenőrző, úgynevezett perifériavezérlő számítógépeket a korlátozott (általában legfeljebb néhány kilométeres) állítási távolság miatt célszerű a vezérelt és ellenőrzött elemek közelében, **decentralizáltan** elhelyezni. Az irányító központ területéhez tartozó valamennyi vezérelt és ellenőrzött külsőtéri elem kapcsolatát meghatározó biztosítóberendezési logika és a kezeléseket és visszajelentéseket biztosító számítógépek ugyanakkor értelemszerűen **centralizáltan** helyezkedhetnek el.

A központi és a perifériavezérlő **számítógépek egymás közötti kapcsolatát** pont-pont vagy busz jellegű biztonsági adatátviteli összeköttetések teremtik meg. A külsőtéri elemek működtetéséhez szükséges energiát közvetlenül a perifériavezérlőkhöz vezetik.

Az elektronikus biztosítóberendezések funkcionálisan három szintre tagolhatóak:

- az ún. **kezelői szint,** azaz a kezelő- és megjelenítő felület, a hozzá tartozó illesztő felülettel a biztonsági szint felé; feladata a kezelések fogadása, formai és tartalmi helyességének vizsgálata, valamint a visszajelentések megjelenítése;
- a **biztonsági szint,** melynek feladata
    - a kezelések, illetve az automatikus behatások és az ellenőrzött objektumoktól érkező jelek, valamint a függőségi tervek alapján az elemek közötti biztonsági értékű kapcsolatok létesítése, azaz a vágányúti logika megvalósítása;
    - a kapcsolódó rendszerekkel, pl. a vonatbefolyásolással való együttműködés szervezése;
- az **állítási szint**, amelynek feladata a biztonsági szint számítógépei és a külsőtéri objektumok közvetlen vezérlését és ellenőrzését ellátó elemek közötti illesztés.

A biztonsági értékű feladatokat általában olyan, gyártó-specifikus, de nem feladat-specifikus **biztonsági számítógép magok** oldják, meg amelyek tetszőleges információk biztonsági jellegű feldolgozására alkalmasak.

Az elektronikus biztosítóberendezéseknél általában valamennyi rendszerkomponenst (a számítógépelemeket és az interfész jelfogóit is) azonos kialakítású, dugaszolható modulokra építve helyezik el. Ezek a modulok szabványosított fiókokban, illetve szekrényekben helyezkednek el, és a szekrényen belül nyomtatott huzalozású hátlapok (backpanelek) kötik őket össze. A szekrények kapcsolatát rendszerkábelekkel oldják meg.

Ez a rendszerfelépítés lehetővé teszi, hogy a teljes berendezést már a gyárban összeállítva levizsgálják, ami a helyszíni szerelési, ellenőrzési munkák lényeges csökkenését eredményezi.

A vágányúti logika

A vágányúti logika az elektronikus rendszereknél többnyire **vágányúti elven**, a függőségi táblázatok (menetterv, elzárási terv) alapján épül fel. A táblázatokban megjelenik a vágányút teljes leírása: minden egyes vágányúthoz hozzárendelik a vágányútban érintett valamennyi külsőtéri elemet, mégpedig az érintettség módjának megadásával. A táblázatok minden egyes vágányúthoz meghatározzák a jelző szabadra állításának feltételeit, a szabad jelzési kép fogalmat, valamint a vonat általi, üzemszerű, elemenkénti oldás feltételeit.

A rendszerek egy kisebb részénél az egyes külsőtéri elemekhez (váltó, jelző stb.) tartozó funkciókat az elem típusának megfelelő szoftver modulok teljesítik, és a vágányúti logika **nyomvonal elven**, ezeknek a moduloknak a vágányhálózatnak megfelelő kapcsolata, az ún. modul-, illetve elemkapcsolati tervek alapján épül fel. A nyomvonal elvű vágányúti logika előnye, hogy helyszínrajzi változások esetén csupán az elemkapcsolati rendszert kell aktualizálni.

Egyes, kifejezetten kisebb állomásokra szánt berendezés típusoknál valamennyi függőséget, így a vágányúti logikát is a **Boole-algebra** segítségével fogalmazzák meg.

A vágányúti logika fajtájától függetlenül, a nagyobb üzemi rugalmasság érdekében a vágányutak feloldása elemenként történik, a jelfogós berendezéseknél is ismert működési sorrendi feltételek teljesülésének figyelembevételével.

Szoftverstruktúra

Az elektronikus biztosítóberendezések szoftvere három részből áll:

- az alkalmazás-független **alapszoftver** vagy rendszer-szoftver, amely
  - szokásos módon szervezi az egyes számítógépek alapvető működését, a feldolgozó, az I/O és az egyéb műveletek végrehajtását, valamint
  - gondoskodik azokról a funkciókról, amelyek a számítógépek biztosítóberendezési alkalmazásához szükségesek, mint például
    - a szoftver és a hardver elemeknek a számítógépek bekapcsolása utáni és programfutás közbeni vizsgálata,
    - a rendszerben szereplő számítógépek együttműködése,
    - a biztonsági adatcsere és adatátvitel az egyes számítógépek között stb.;
- a **biztosítóberendezési funkciókat** megvalósító, az alkalmazásorientált specifikumokat, így a felhasználó vasút előírásait is tartalmazó szoftver, amely általában moduláris felépítésű;
- a konkrét **alkalmazási eset** adatait, azaz a konfigurációs adatokat, illetve az adott állomás biztosítóberendezési elemeinek tervezési adatait, többnyire táblázatos formában tartalmazó rész.

A szoftver ilyen módon való felépítése, illetve tagolása és a **kölcsönös elfogadás** (cross-acceptance) elvének következetes alkalmazása együttesen lehetővé teszi a biztonsági elfogadási/jóváhagyási eljárások lényeges egyszerűsödését.

Az alapszoftver **generikus** jellegéből adódóan, elegendő azt az első alkalmazás előtt a megfelelő hatósággal elfogadtatni, és bármely vasútnál való további alkalmazás már nem igényel újabb elfogadást.

A biztosítóberendezési funkciókat megvalósító szoftver általában

- egy **generikus**, a valamennyi vasúttársaságnál azonos módon alkalmazható funkciókat tartalmazó, és
- egy **generikus alkalmazási**, az egyes vasutak specifikumait tartalmazó, egyes esetekben táblázatos formában megvalósított

részre bontható. Ez a felbontás lehetővé teszi, hogy a generikus részt az alapszoftverhez hasonlóan csak a rendszer első alkalmazása előtt kelljen elfogadtatni, a generikus alkalmazási részt pedig csak az egyes vasutaknál történő első alkalmazás előtt, illetve meglévő alkalmazásnál a forgalmi-üzemi előírások változása esetén.

Az egyes berendezések adatait tartalmazó rész **specifikus alkalmazási** jellegű, így ezt a részt minden egyes berendezés esetében külön-külön el kell fogadtatni.

2. Az elektronikus biztosítóberendezések biztonsága [3],[5]

A mikroelektronikai elemek teljesen más tulajdonságokkal rendelkeznek, mint a korábban alkalmazott biztosítóberendezési jelfogók. Ezért az alapvetően nem biztonsági alkalmazásra fejlesztett mikroelektronikai elemek biztonsági rendszerekben való alkalmazhatósága érdekében

- meg kellett találni azokat az új rendszerstruktúrákat és módszereket, amelyek révén a szükséges biztonsági és rendelkezésreállási szint elérhetővé vált;
- ki kellett dolgozni azokat az új technikának megfelelő biztonságigazolási módszereket, eljárásokat, amelyek révén a kívánt biztonsági és rendelkezésreállási szintek elérése igazolható.

Az elektronikus biztosítóberendezések biztonsága lényégében a következő tényezők alkalmazásával valósul meg:

- biztonsági számítógépek,
- biztonsági adatátvitel az egyes számítógépek között,
- a különleges kezelésekhez információt szolgáltató visszajelentések biztonsági értékű megjelenítése,
- a különleges kezelések biztonsági jellegű végrehajtása,
- helyes működésű szoftver.

A mikroelektronikai elemek tulajdonságai és az azoknak megfelelő hibafeltáró és hibakezelő eljárások alapján, a mikroelektronika és a számítástechnika lehetőségeinek felhasználásával, a legkülönbözőbb fejlesztési, rendszertechnikai és alkalmazási megoldások alakultak ki a biztonsági felelősségű rendszerek számára.

Valamennyi megoldás tartalmaz egy, a gyártó cégre jellemző ún. **biztonsági magot**, amely a hardver és a szoftver megfelelő együttműködése alapján, a bemeneti információk adott algoritmus szerinti biztonsági feldolgozását és a feldolgozás eredményének a kimeneteken való megjelenítését végzi. Ez a biztonsági mag alkalmazás-független módon van kialakítva, így tetszés szerinti biztonsági vezérlő és ellenőrző feladatra alkalmazható.
A biztonsági magot úgy kell kialakítani, hogy képes legyen a biztonsági rendszerben üzem közben **véletlenszerűen** fellépő hardver hibák (meghibásodások) észlelésére, és a szükséges biztonsági reakciók kiváltására.
A biztonsági rendszerek hardverének és szoftverének fejlesztése, tervezése, gyártása és üzemeltetése során elkövethető **emberi eredetű** hibák a rendszer működése során, bizonyos működési állapotokban rendszeresen kifejtik hatásukat. Ezért szokták ezeket **szisztematikus** hibáknak nevezni. Egy felismert és eltávolított szisztematikus hiba nem léphet fel újra. Nagy szoftver rendszerekben azonban könnyen előfordulhat, hogy a hiba eltávolításakor újabb szoftverhiba kerül a rendszerbe. A szisztematikus hibák, illetve hatásuk elleni védelem két alapvető módszere

- a hibakizárás és
- a hibakövetkezmények kizárása.

A következőkben röviden áttekintjük a véletlenszerű és a szisztematikus hibák elleni védelem alapjait.

A véletlenszerű hardver hibák veszélytelensége

A jelfogós technikához hasonlóan itt is érvényes az, hogy az egyszeres hibáknak nem szabad veszélyes állapothoz vezetniük. A nagyintegráltságú elemek (processzorok stb.)

tulajdonságainak megfelelően azonban a hibaanalízis és a hibakövetkezmény-analízis nem az alkatrészek, hanem az egyes funkciócsoportok szintjén hajtható végre, és eredményként is az egyes funkciócsoportokat (pl. nyomtatott áramköri kártyákat) minősítjük hibátlannak vagy hibásnak. Megjegyzendő azonban, hogy redundancia, illetve megfelelő referencia nélkül nem ismerhető fel, hogy a funkciócsoport hibátlanul működik-e.

A biztonsági információk redundáns, hardveresen **kétcsatornás** feldolgozására mutat példát az 1. ábra. A két, hardveresen és szoftveresen is azonos funkciócsoport ugyanazokat a bemenő jeleket kapja és dolgozza fel. A kimenetükön megjelenő vezérlőjeleket biztonsági (2-ből 2) összehasonlító hasonlítja össze egymással. Amennyiben a két csatornán érkező jel azonos, az összehasonlító kimenetén megjelenik a most már biztonsági értékű vezérlőjel. Amennyiben az összehasonlító, az egyik csatornában fellépő hardver hiba miatt, a két csatorna jelei között eltérést tapasztal, letiltja a biztonsági kimenetet.

A redundáns feldolgozás másik alapeseténél az előbbi rendszer kiegészül egy harmadik csatornával (2. ábra). A három csatorna kimenő jeleit egy ún. 3-ból 2 **többségi** vagy **szavazó** logika értékeli ki, amelynek a kimenetén akkor jelenik meg a biztonsági értékű vezérlőjel, ha legalább két csatorna kimenő jele azonos volt. Ez azt jelenti, hogy az egyik csatornában fellépő hiba ellenére a rendszer még továbbra is biztonságosan működik, azonban a meghibásodott csatorna kimenő jelét a csatorna helyreállításáig a további szavazásoknál nem szabad figyelembe venni. Az ilyen konfigurációk nemcsak biztonságosak, hanem egyszeresen **hibatűrőek** is.

A redundáns módon felépített (többcsatornás) rendszerek biztonságához teljesülniük kell a következő feltételeknek:

- az összehasonlítás, illetve a szavazás mindenképpen biztonsági jellegű kell, hogy legyen, tehát saját hibáját is fel kell fedje;
- a redundáns részrendszereknek (csatornáknak) biztonsági szempontból egymástól függetleneknek (csatolásmentesnek) kell lenniük, különben az egyik csatornában fellépő hiba azonos hibaállapotokat okozhatna valamennyi csatornában;
- az egyszeres hibák feltárása és a megfelelő hibareakció kiváltása megfelelően gyors kell, hogy legyen, különben az egyes csatornákban azonos hibaállapotokat okozó véletlenszerű többszörös meghibásodások valószínűsége már nem tekinthető elhanyagolhatónak.

A megengedett hibafeltárási idő betartása érdekében nemcsak folyamatfüggő (adatáramlás-függő), hanem folyamattól független (adatáramlástól független), ciklikus vizsgáló rutinokon alapuló eljárásokat is alkalmaznak.

Hibakizárás

A hibakizárás módszerének lényege az, hogy a biztonsági rendszer életciklusa során, különösen a fejlesztési fázisban elkövethető hibákat gondos, megfelelő minőségű munkával elkerüljék, illetve a rendszerbe mégis bekerült hibákat a megfelelő pontokon végzett, átfogó ellenőrzésekkel, teszteléssel még az üzembe helyezés előtt feltárják és kijavítsák, végül az üzembe helyezendő rendszer hibamentességét megfelelő módszerekkel bizonyítsák.

A szoftver tervezésével, kialakításával, dokumentálásával és vizsgálatával kapcsolatos előírásokat az MSZ EN 50128 szabvány tartalmazza. Az előírások annál szigorúbbak, minél magasabb a biztonsági osztály.

A szoftverhibák elkerülése nagyon tudatos, körültekintő szoftverfejlesztési tevékenységet igényel. Sajnos azonban, a leggondosabb fejlesztés esetén is kerülhetnek hibák az új szoftverekbe. Éppen ezért a szoftverfejlesztés alapos, szoftver eszközökkel segített, független

(befolyásolástól mentes) vizsgáló által történő ellenőrzésének rendkívül nagy a jelentősége a hibafeltárás, és ezzel a szoftver hibamentessége szempontjából.

A hibakövetkezmények kizárása

Ezeknél a rendszereknél abból indulnak ki, hogy a szoftver tervezése során keletkező hibák teljes mértékben nem zárhatóak ki, azonban ezeknek a hibáknak a veszélyes következményeit mindenképpen ki kell zárni vagy el kell kerülni. Ennek egyik lehetősége az ún. **szoftver-diverzitás**, azaz egymástól eltérő szoftverek tervezése, aminek révén a szoftver hibák, a különböző programcsomagok futáseredményei közötti eltérések révén felfedhetőek. A biztonság szempontjából hardveresen egycsatornás rendszerben a két szoftvercsomag aktuális részei egymás után kerülnek feldolgozásra. Az eredmények ezt követő összehasonlítása hardveresen vagy szoftveresen történhet.

A diverz szoftverek fejlesztése szintén nagyon gondos szervező és programozási munkát feltételez, annak érdekében, hogy a két szoftvercsomag kívánt diverzitása ne csak létrejöjjön, hanem bizonyítható is legyen.

A szoftver alapú biztonsági rendszerek egy különleges osztálya az ún. **eljárásbiztonságon** alapul. Ezeknél a rendszereknél a tulajdonképpeni felhasználói szoftvert speciális, a teljes rendszert állandóan ellenőrző vizsgálószoftverrel egészítik ki: meghatározott felépítésű és tartalmú vizsgálószavak cirkulálnak állandó jelleggel és igen szigorú időbeli előírásokkal, valamennyi modul érintésével. Ezáltal vizsgálják a biztosítóberendezési szoftver rendeltetésszerű futását és a hardver megfelelő működését. Hiba vagy zavar feltárása esetén a biztonsági lekapcsolás révén gyakorlatilag azonnal lekapcsolódik a be- és kimeneti kártyák áramellátása, és ezzel blokkolódik az egész biztonsági rendszer.

A biztonsági rendszerek szoftverének fejlesztése nagyon munkaigényes és költséges. Hibakizárási eljárás esetén nagy ráfordítást igényel a gondos szoftvertervezés, a hibafeltárás és -eltávolítás, valamint a szoftver hibátlanságának igazolása a **fejlesztési** fázisban. A hibakövetkezmények kizárása esetén a nagyobb ráfordítás a kétszeres szoftvertervezés révén keletkezik, aminek az eredménye még mindig nem feltétlenül hibamentes. Így ennél az eljárásnál a hibák feltárása és eltávolítása részben az **üzemeltetési** fázisba kerül át.

A gyakorlatban mindkét eljárást alkalmazzák. A biztosítóberendezési ipar és a vasúttársaságok felfogása megoszlik annak vonatkozásában, hogy a két eljárás közül melyik alkalmasabb a szoftverhibákból adódó veszélyes állapotok elkerülésére.

3. A kezelő és visszajelentő rendszer [1],[2],[3]

Az elektronikus biztosítóberendezések kezelőkészülékét, vagy más néven kezelőfelületét, illetve kezelői munkahelyét az egyes vasutak követelményeinek megfelelően alakítják ki. Egy-egy kezelői munkahelyről több biztosítóberendezés is kezelhető, más esetekben pedig egy-egy biztosítóberendezéshez több kezelői munkahely is tartozhat. Amennyiben a kezelendő körzet nagyságából adódóan ugyan elegendő egy munkahely, a rendelkezésreállás érdekében mégis gyakran létesítenek egy második munkahelyet is, amelyet kiképzési, ellenőrzési, bemutató és karbantartási célokra is lehet használni.

Egy kezelői munkahely minimum a következő elemekből áll:

- a kezelések bevitelére alkalmas készülék (fényceruza, grafiktablett, billentyűzet, manapság elsősorban egér, ritkábban hagyományos nyomógombos kezelőkészülék);
- visszajelentő készülék (nagy felbontású, nagy képernyős, színes monitor és/vagy kivilágított vágánytábla);
- nyomtató, a számítógépes rendszer által regisztrált kezelések, események kívánság szerinti kinyomtatására.

Nagyobb kezelési körzetek esetén természetesen egy-egy kezelői munkahelyhez több monitor is tartozhat.

A korszerű kezelői munkahelyekre jellemzői a következők:

- világos folyamatmegjelenítés teljes grafikával és ablak-technikával, nagy felbontású, színes monitorokon;
- kényelmes kezelhetőség egérvezérlésű kurzorral, közvetlenül a vágányábrában, menüvezérléses, magától értetődő kezeléssel, a téves kezelések lehetőségének csökkentésére;
- a gyakran előforduló, rendszeres kezelési műveletek egyszerűsített (pl. kettős kattintással) való végrehajtásának lehetősége;
- számos rendszerfunkció a kezelések támogatására és a karbantartáshoz;
- nagyfokú rendelkezésreállás a redundáns rendszerfelépítés révén;
- nagyfokú biztonság a különleges kezelési műveletek számára.

Egyes rendszerek a képernyőn a vágányábrán kívül szöveges információt tartalmazó, ún. **üzenetkezelő** ablakokat is megjelenítenek, a következő funkciók számára:

- kezelési felhívások (pl. „Jelzőt kezelni”),
- üzemi jelentések (pl. egy kezelés visszautasítása),
- a biztosítóberendezés zavarai részletezettebb módon, és
- rendszerjelentések, a kezelői munkahely elemeinek állapotáról, pl. hibakeresés céljára.

A jelzések, nyugtázhatók, törölhetők, szükség szerint ismételten megjeleníthetők, és tartozhat hozzájuk figyelmeztető hangjelzés is.

A képernyős megjelenítésnél megkülönböztetjük

- a teljes kezelési körzet állapotát ábrázoló, viszonylag kevés, de a normál kezelések kiadásához elegendő részletet tartalmazó, **áttekintő képeket,** és
- az egyes kiválasztott részterületek minden információját megjeleníteni képes ún. **lupe képeket.** A különleges kezelések kiadásának előfeltétele a kezelő megfelelően részletes és korrekt informáltsága, ezért ezek a kezelések általában csak a lupe képek alapján adhatóak ki.

A vasutak egy része ragaszkodik ahhoz, hogy a kezelőkészülékek is biztosítóberendezési szintű biztonsággal legyenek kialakítva, míg más vasutak ezt nem igénylik. Ez utóbbi természetesen teljesítményveszteséggel jár, mert az üzemi vagy berendezési eredetű zavarok esetén szükséges különleges (biztonsági igényű) kezelések parancsai a nem biztonsági szintű kezelőkészülékről nem, vagy csak korlátozásokkal (pl. meghatározott időkésleltetés után) adhatóak ki.

A biztonsági igényű, ún. **különleges kezeléseket** az egyéb kezelésekkel azonos módon, a kezelőkészüléken kell kezdeményezni, majd egy ellenőrző visszajelzés megérkezése és kiértékelése után (az fog történni, amit szándékoztunk?), egy az előbbitől független kezelőszervvel (független csatornán) kell a szándékot megerősíteni (különleges kezelés engedélyezése, parancsfelszabadítás). A szándék megerősítése történhet más módon is, például a különleges kezelés meghatározott időn belüli, másodszori, de az elsőtől formájában teljesen eltérő beadásával, az ún. **eljárásbiztonság** elvén.

A **biztonsági megjelenítés** egyik szokásos megoldásánál a kijelzés biztonsága érdekében a monitorképek két, egymástól független információs csatornából származnak, és ezeket kb. 1 másodperces ütemben váltakozva kapcsolják a képernyőre. Zavarmentes esetben, az azonos képek fedése révén, nyugodt kép látható a képernyőn. A két vezérlőegység egyikénél fellépő hiba esetén az érintett képrészlet a képátkapcsolás ütemében villog, és ezáltal a kezelő a hibát felismerheti. A biztonsági megjelenítés egy másik változatánál az egyes csatornákhoz tartozó videomemóriák tartalmát még a megjelenítés előtt összehasonlítják, és csak egyezőség esetén engedélyezik a megjelenítést.

4. A mérnöki munkahely [1],[2],[4]

Az elektronikus biztosítóberendezésekben alkalmazott nagy megbízhatóságú hardverelemek és hibatűrő rendszerstruktúra révén e rendszerek karbantartási és javítási igénye alacsonyabb, mint a hasonló feladatokat ellátó jelfogós biztosítóberendezéseké. Ugyanakkor az elektronikus rendszerekben fellépő hibák helyének és okának megtalálása, valamint a hibás állapot megszüntetése jóval bonyolultabb feladat, mint a jelfogós berendezéseknél, és nemritkán mérnöki felkészültséget igényel. Ez a helyzetet enyhíthető olyan, szerviz és diagnosztikai célú, többnyire PC-alapú, mérnöki munkahelyek (diagnosztikai terminálok) kialakításával, amelyek a felügyelt rendszer minden olyan állapotinformációját begyűjtik, tárolják és megjelenítik, amelyekkel támogatható a szakszerű, minél egyszerűbb és gyorsabb hibafeltárás és -javítás.

Ilyen mérnöki munkahely telepíthető közvetlenül az egyes biztosítóberendezésekhez, például a számítógépterembe, és/vagy megfelelő, akár több tíz vagy száz kilométeres távadat-átviteli kapcsolat kiépítésével, az adott területen működő biztosítóberendezések üzemeltetéséért felelős szervezeti egység székhelyén, központosítottan (távdiagnosztika).

Az elektronikus biztosítóberendezések moduláris felépítése és a részrendszerek közötti, többnyire buszrendszerű összeköttetés, illetve a számítógépek hálózatba kapcsolása révén a központosított (egy munkahelyre koncentrált) hibadiagnosztizálás feltételei lényegesen kedvezőbbek, mint a jelfogós technikában. A biztosítóberendezés szoftvere, beleértve a kiterjedt öndiagnosztizáló programokat is, folyamatosan felügyeli a hardvert és a vele összefüggő funkciókat. Ennek alapján folyamatosan állapotjelzések (hibaállapot esetén

hibajelzések is) kerülnek továbbításra a diagnosztikai számítógéphez, amely kiértékeli a kapott információkat, és kijelzi, illetve kívánságra ki is nyomtatja a kiértékelés eredményét.

A kiértékelést segíti, hogy a mérnöki munkahely számítógépe, egy adott, hosszabb időszakra vonatkozóan, a kezelőfelület teljes adatforgalmát (kezelések és visszajelentések) is tárolja. Így valamely hibaesemény bekövetkezésekor a hibát megelőző események is ismertek. A megjelenített állapotinformációk, a könnyebb értelmezhetőség érdekében, többnyire szöveg formátumúak.

A mérnöki munkahelyek egy része lehetőséget kínál interaktív tevékenységre is; például lehetővé teszi a számítógépek tártartalmának lekérdezését, ami a hibajelenségek okának megállapításában nyújthat hatékony segítséget.

A mérnöki munkahelyre központosított diagnosztikai információk mellett az egyes számítógép és periféria modulok előlapjain található hexadecimális és/vagy bináris (LED) kijelzők lehetővé teszik az elektronikai egységek állapotának helyben történő kiértékelését is. Egyes rendszerekben a számítógépek e célra külön diagnosztikai kiértékelő és kijelző modullal is rendelkeznek.

5. Elektronikus biztosítóberendezések Magyarországon

Az elektronikus biztosítóberendezések korábban bemutatott alapstruktúrája a gyakorlatban számos gyártóspecifikus variációban valósul meg. Ezek főként az alkalmazott biztonsági és rendelkezésreállási koncepcióban, valamint a berendezések hatókörzetének nagyságában különböznek egymástól. A következőkben azokat a rendszereket mutatjuk be röviden, amelyek Magyarországon a jelen Kézikönyv írásának időpontjáig alkalmazásra kerültek.

ESTW MÁV (Siemens, SIMIS C) [1]

A MÁV Rt. első elektronikus biztosítóberendezése 1997 márciusa óta van üzemben a Budapest-Hegyeshalom vasútvonal Tata állomásán. A rendszer a SIMIS biztonsági számítógépek (**Si**cheres **Mi**krocomputer-**S**ystem von Siemens – a Siemens biztonsági mikroszámítógép-rendszere) alkalmazására épül.

A SIMIS-elv szerint kialakított számítógépek két, egymástól független, azonos felépítésű mikroszámítógépből állnak (3. ábra). A két gép kicseréli egymás közt a bemeneti adatokat. Amennyiben mindkét adatcsomag azonos, a megfelelő csatornák feldolgozzák ezeket.
A két feldolgozó csatornán ugyanaz a szoftver fut, és órajelük is közös, így a két csatorna egyidejűleg ugyanazokat a műveleteket végzi el. Ezzel a módszerrel hibátlan esetben a perifériaegységek számára adott kimeneti parancsoknak meg kell egyezniük. A feldolgozás eredményei csak akkor kerülnek kiadásra, ha a két csatorna eredményei megegyeznek (2-ből 2 elv). Eltérés esetén az összehasonlítók átkapcsolják a kimeneteket biztonsági, akadályozó állapotba (biztonsági lekapcsolás).
A mikroszámítógépek helyes működését kiegészítő, rendszeresen lefutó vizsgálóprogramok ellenőrzik. Ez a módszer lehetővé teszi, hogy a még fel nem fedett hibák is észrevehetőkké váljanak. Mihelyt az első hiba felismerhetővé vált, a 2-ből 2 rendszer a folyamat irányában inaktívvá válik. Ez megakadályozza, hogy egy esetleg fellépő második hiba veszélyes hatással lehessen a folyamatra.
Amennyiben nagyobb rendelkezésreállásra van szükség, az 2x(2-ből 2) elrendezés révén biztosítható. Ebben az esetben két SIMIS-számítógépegység működik, amelyek mindegyike

2-ből 2 konfigurációjú. Az egyik az aktív, a másik a tartalék számítógép. A két számítógép közül mindkettő elvégzi a folyamatadatok feldolgozását, de csak az egyik vesz részt ténylegesen a folyamat irányításában. Ha ez a számítógép kiesik, a rendszer a másik, ugyancsak 2-ből 2 elvű egységre, a tartalék számítógépre kapcsol át. Ennek az elrendezésnek az előnye különösen a biztosítóberendezések módosításakor és kiegészítéseinél jut érvényre: amíg a tartalék számítógépet módosítják, az aktív számítógép akadályoztatás nélkül működhet tovább.

A számítógépek feladatai

Tata állomás elektronikus biztosítóberendezésében a különböző feladatok ellátására a SIMIS-számítógépek három, különböző típusát alkalmazzák (4. ábra):

- az EKIR beviteli, ellenőrző és értelmező számítógép,
- az SSR illesztő-számítógép és
- a BSTR körzeti (állító) számítógépek.

Az **EKIR** a következő feladatokat látja el:

- elvégzi a több számítógépes biztosítóberendezési rendszer központi irányítási, összehangoló feladatait,
- tárolja az összes berendezés-specifikus adatot,
- üzembevételkor vagy egy számítógép újraindítása esetén ellátja a körzeti (állító) számítógépeket a berendezés-specifikus adatokkal (például elemcímek, körzetfelosztás, kapcsolatok a szomszédos elemekkel, az elemek program-esetei),
- a körzeti (állító) számítógépekkel folytatott információcsere útján vezérli a vágányutak felépítését,
- tartja a kétirányú kapcsolatot az ILTIS kezelő és visszajelentő rendszerrel:
- átveszi a kezelői utasításokat, feldolgozza azokat, és végrehajtásra továbbítja a körzeti (állító) számítógépeknek,
- a körzeti (állító) számítógépektől érkező folyamatállapot információkat továbbítja az ILTIS rendszernek,
- a rendszerrel kapcsolatos átfogó és részletes információkkal látja el a diagnosztikai számítógépet.

Mivel az EKIR központi feladatot lát el a biztosítóberendezésben, a megbízhatóság érdekében 2x(2-ből 2) redundáns felépítésű.

Az **SSR** illesztő-számítógép. Feladata lényegében a back-up (biztonsági tartalék) számítógépé. Tárolja az összes folyamatállapot-adatot és kezeléseket, annak érdekében, hogyha valamelyik körzeti számítógépnél újraindításra van szükség, az aktuális adatok rendelkezésre álljanak. A SIMIS rendszer más alkalmazásainál feladata a kezelő-visszajelentő rendszerrel való kapcsolattartás is. Ekkor szokásos jelölése: BAR. Az SSR, az EKIR-hez hasonlóan, redundáns felépítésű.

A **BSTR** körzeti (állító) számítógépek mindegyikéhez a külsőtéri berendezések egy-egy meghatározott csoportja van hozzárendelve. Tata állomáson a BSTR számítógépek redundancia nélküli 2-ből 2 kiépítésben működnek. Ezek a gépek

- üzembe állításukkor megkapják a hozzájuk rendelt körzetekben a feladataik ellátásához szükséges elemadatokat,
- kapcsolatot tartanak más BSTR-ekkel, ha azok valamely vágányút képzésében és felügyeletében az adott BSTR-rel együtt vesznek részt,

- végzik a tulajdonképpeni állítási műveleteket, így a vágányutak beállítását, felügyeletét és feloldását,
- vezérlik az STT állítóegységeket,
- feldolgozzák az egyes külsőtéri elemek, így a váltók és jelzők állapotáról érkező információkat,
- ciklikusan ellenőrzik a külsőtéri objektumok szabályszerű működését.

A jelzők és a váltók közvetlen vezérlése és ellenőrzése az elektronikus, illetve jelfogós felépítésű **STT** állítóegységek révén valósul meg. A többi külsőtéri objektum és kapcsolódó rendszer a BSTR-ek digitális I/O pontjaira csatlakozó külső interfész áramkörökön keresztül csatlakozik a számítógépes rendszerhez.

A **75 Hz-es sínáramkörök** és a sugárzókábelek ütemezett jellel történő táplálásának vezérlésére a tatai berendezésnél a megfelelő körzeti számítógépekkel párhuzamos interfészen keresztül kapcsolatot tartó, SIMATIC S5-115F típusú, kétcsatornás biztonsági logikai vezérlőket (PLC-ket) alkalmaznak.

Az egyes számítógépek közötti információátvitel számára a teljes kezelési körzetet átfogó **biztonsági buszrendszer** szolgál, amely a rendelkezésreállás növelése érdekében kettőzött, redundáns felépítésű. Az információátvitel egyidejűleg mindkét buszrendszeren, biztonsági kódolással ellátott módon történik. Valamelyik buszrendszer kiesése esetén a rendszer zavartalanul, biztonságosan működik tovább, a megmaradt buszrendszeren továbbított, kettőzött hosszúságú táviratok révén. Az egycsatornás biztonsági átviteli üzemmód megengedett időtartamát, egy további hiba kedvezőtlen hatásának megelőzése érdekében, a vasutak általában néhány órára korlátozzák.

A rendszer **vágányúti logikája** nyomvonal elvű, és ennek megfelelően az elemkapcsolati terven alapul.

A tatai berendezésnél a kezelések és visszajelentések számára az elsősorban Svájcban, de más országokban is igen elterjedt **ILTIS** rendszert alkalmazták. A MÁV Rt. veresegyházi vonalán ILTIS rendszer távvezérli Veresegyház állomásról a Rákospalota-Újpest – Vácrátót szakasz állomásainak jelfogós biztosítóberendezéseit. Az ILTIS rendszernél a megjelenítés biztonságát a képernyő memóriák tartalmának visszaolvasásával és összehasonlításával érik el.

ELEKTRA (Alcatel Austria) [2]

Az ELEKTRA rendszer (5. ábra) az első, Almásfüzítő-felső állomáson történt telepítése óta a MÁV Zrt. és a GYSEV számos állomásán, valamint a BKV-nál is több helyen (HÉV vonalakon) került alkalmazásra. A rendszer különleges biztonsági koncepciót alkalmaz, amely Safety Bag (biztonsági csomag) néven vált ismertté. A biztonsági követelmények teljesítéséhez a biztosítóberendezés minden biztonságreleváns működése alapvetően kétcsatornás feldolgozású.

A kezelő által beadott parancsokat először a **logikai csatornában** az üzemi és a biztonsági feltételeknek megfelelően ellenőrzik, és ha az eredmény pozitív, a parancskiadást a külsőtéri elemek vezérléséhez előkészítik. A vezérlés kiadása előtt azonban visszakérdeznek az előbbitől független **biztonsági csatornára**, annak ellenőrzésére, hogy a logikai csatorna

eredménye valóban nem vezet-e veszélyes állapothoz (Safety Bag eljárás). Csak akkor adja ki mindkét csatorna az állítási parancsokat a megfelelő jelfogós interfészre, ha ez a feldolgozás is eredményes volt. Az interfészen megtörténik a két parancs ismételt, hardveres összehasonlítása, mielőtt ténylegesen végbemenne a külsőtéri elemek vezérlése.

A rendelkezésreállás megfelelő szintjének elérése érdekében mindkét csatornát hibatűrő módon alakították ki: A központi számítógépek háromszoros, a perifériavezérlő és a kezelői számítógépek pedig kétszeres kiépítésűek.

Az egyes **számítógépek pont-pont közötti összeköttetések** révén kapcsolódnak egymáshoz. A nagyobb rendelkezésreállás érdekében az összekötetések megkettőzhetőek. A távolabb fekvő folyamatperifériákkal való kapcsolattartás érdekében a központi számítógép és a perifériavezérlő közé egy X.25-ös átviteli út iktatható be, amely megfelelő intézkedésekkel nagyobb távolságú biztonsági információátvitelt is lehetővé tesz.

Az ELEKTRA rendszerben a hardver és a szoftver biztonsági követelmények teljesítése érdekében a két független hardver csatornán **diverz** (eltérő) **szoftvereket** futtatnak. A két szoftver diverzitását a következőkkel érik el:

- eltérő specifikáció a két, különböző feladatot ellátó csatorna részére.
- eltérő programnyelvek a két csatorna számára
    - a logikai csatorna a programjait CHILL (CCITT High Level Language – CCITT Magas Szintű Nyelv) programnyelven írták. A CHILL folyamatorientált, magas szintű nyelv. Algoritmikus elemei a Pascal-hoz hasonlóan vannak definiálva, és tartalmazza a valósidejű alkalmazásokhoz szükséges nyelvi szerkezeteket is;
    - a biztonsági csatornában használt szabályorientált programnyelv a PAMELA (PAttern Matching Expert system LAnguage – mintaillesztő szakértő rendszeri programnyelv).

A központi számítógépeknél az e célra kifejlesztett VOTRICS (Voting-Triple-Modular-Computing-System – háromszoros szavazó moduláris számítógép rendszer) eljárással oldják meg a 3-ból 2 jellegű működést, azaz hogy egy számítógép meghibásodásakor még nem lép fel a rendszer funkcionalitásának korlátozása. A kettőzött, perifériavezérlő és kezelői számítógépek melegtartalékolt üzemmódban működnek, azaz mindkét számítógép folyamatosan megkapja az információkat, azonban az irányításban egyidejűleg csak az egyik vesz részt. Ennek meghibásodása esetén a másik gép gyakorlatilag megszakítás nélkül képes átvenni az irányítást.

A **vágányúti logika** vágányutas elvű, függőségi táblázatokon alapul. A **visszajelentések megjelenítése** az állomásnagyságtól függően egy vagy több képernyőn, kizárólag lupeképként, képváltásos módszerrel, biztonsági jelleggel történik. A kezelés alapvető eszköze az egér.

SIMIS IS (Siemens) [4]

A SIMIS IS rendszert eredetileg kis és közepes méretű állomások számára fejlesztették ki. Első alkalmazására Magyarországon a MÁV Zrt. Cegléd állomásán került sor. A rendszer egy másik változatának, a SICAS rendszernek első magyarországi alkalmazására a budapesti

metró 2. vonalának felújítása keretében kerül sor. A SIMIS IS rendszer az ECC (Element Control Computer) biztosítóberendezési számítógépekre épül. Az ECC részét képezi:

- a processzorkártyákat és a kommunikációs kártyát tartalmazó feldolgozó egység,
- a perifériavezérlő és interfész egységek, valamint
- az energiaellátó egységek.

A feldolgozó egység

A **processzorkártya** egy gyors, 32 bites processzorral van ellátva. Mindegyik ECC-nek legalább két processzorkártyája van, amelyek ugyanazt az információt dolgozzák fel, órajel szinkronban (2-ből 2 rendszer). A rendelkezésreállás növelése érdekében a feldolgozó egység bővíthető egy újabb processzorkártyával, így támogatva egy 3-ból 2 konfigurációt. Ez azt jelenti, hogy a SIMIS IS megszakítás nélkül dolgozik akkor is, ha az egyik processzorkártya meghibásodik.

A **kommunikációs kártya** köti össze a rendszeren belül az egyes számítógépeket, ezáltal biztosítva az adatcserét. Az adattovábbítás alapja a biztonsági kódolással és megfelelő protokollal működő, ipari szabványú PROFIBUS. A rendelkezésre állás növelése érdekében a busz redundánsan van kialakítva. A központi (biztosítóberendezési) szint és a kezelői szint (a kezelőfelület és a szerviz- és diagnosztikai rendszer) közötti kapcsolatok ugyanezt az adattovábbítási eljárást használják.

Perifériavezérlő és interfész egységek

A váltóhajtóművek és a jelzők energiával való ellátására, vezérlésére és ellenőrzésére az ECC-be integrált elektronikus perifériavezérlők szolgálnak.

További külsőtéri elemek, rendszerek (vágányfoglaltság, útátjáró, vonali berendezések stb.) közvetlen, vagy illesztőegységen keresztüli csatlakozását teszik lehetővé a szintén az ECC-be integrált univerzális digitális bemenet/kimenet vezérlő egységek.

Rendszerkonfiguráció

A rendszer központi részét képezi a kezelő és megjelenítő interfész, valamint a biztosítóberendezési logika (6. ábra).

A **kezelő és megjelenítő interfész** (Operator and Diagnostic Interface – ODI) biztosítja a kapcsolatot a SIMIS IS biztosítóberendezés és a kezelői szint között. Az ODI az alábbi funkciókat végzi:

- biztosítja a kezelőfelületen megjelenítendő, illetve a diagnosztikai rendszer számára szükséges információk tárolását, így a megjelenített információk hűen tükrözik a biztosítóberendezés mindenkori állapotát;
- kezeli és koordinálja a kezelési körzeteket, és kiosztja az egyes kezelőfelületi munkahelyekhez tartozó jogosultságokat;
- kezeli és felügyeli a biztosítóberendezéssel összefüggő kezeléseket;
- működteti a központi biztosítóberendezési órát, továbbítva az időadatokat az alrendszerek óráinak.

A biztosítóberendezési funkciók a **biztosítóberendezési logikába** vannak beépítve. A vágányúti funkciók **táblázatos elven** kerülnek megvalósításra. A megfelelő vágányúti logika kialakítása érdekében az egyes elemekkel kapcsolatos funkciók logikailag össze vannak kapcsolva a vágányúti táblával. Az elem-funkciók felelősek az egyes elemekre vonatkozó egyéni parancsok végrehajtásáért, az adott külsőtéri elem vezérléséért és ellenőrzéséért.

A SIMIS IS biztosítóberendezési rendszer **több-számítógépes** változatában az egyes, hibatűrő (fault-tolerant), 3-ból 2 konfigurációjú ECC számítógépek a biztosítóberendezés hatókörzetébe tartozó külsőtéri elemek és csatlakozó rendszerek egy-egy csoportját vezérlik és ellenőrzik. A biztosítóberendezési logikát ebben az esetben az ECC-kel kapcsolatban álló,

nagyteljesítményű SIMIS PC-k működtetik, nagy rendelkezésreállású, 2 × (2-ből 2) kialakításban.

Felhasznált irodalom

[1] Antweiler, B., W. Staab, Tarnai G.: A Siemens elektronikus biztosítóberendezése Tatán; Vezetékek Világa ’97/3 pp. 20-23.

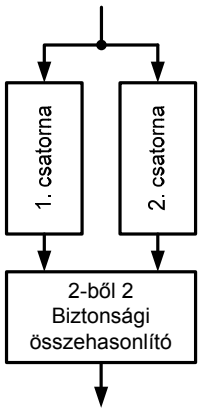
[2] Berger, J.: Das elektronische Stellwerk ELEKTRA; Signal und Draht 84 (1992) 9, pp. 260-263.

[3] Fenner, W., P. Naumann: Verkehrssicherungstechnik; Publicis MCD Verlag, Erlangen und München, 1998. p. 269.

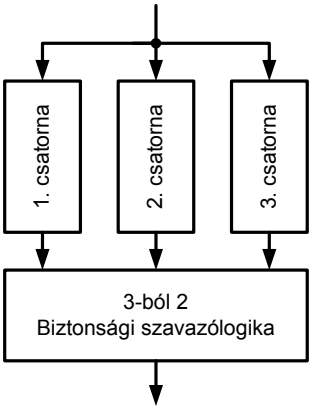
[4] Keller, B.: SIMIS IS – Innovationen für den weltweiten Stellwerkseinsatz; Signal und Draht (94) 9/2002 pp. 26-29.

[5] Tarnai G.: Közlekedési automatika> BME Közlekedésautomatikai Tanszék, Budapest, 2002. www.kka.bme.hu/~kozlaut

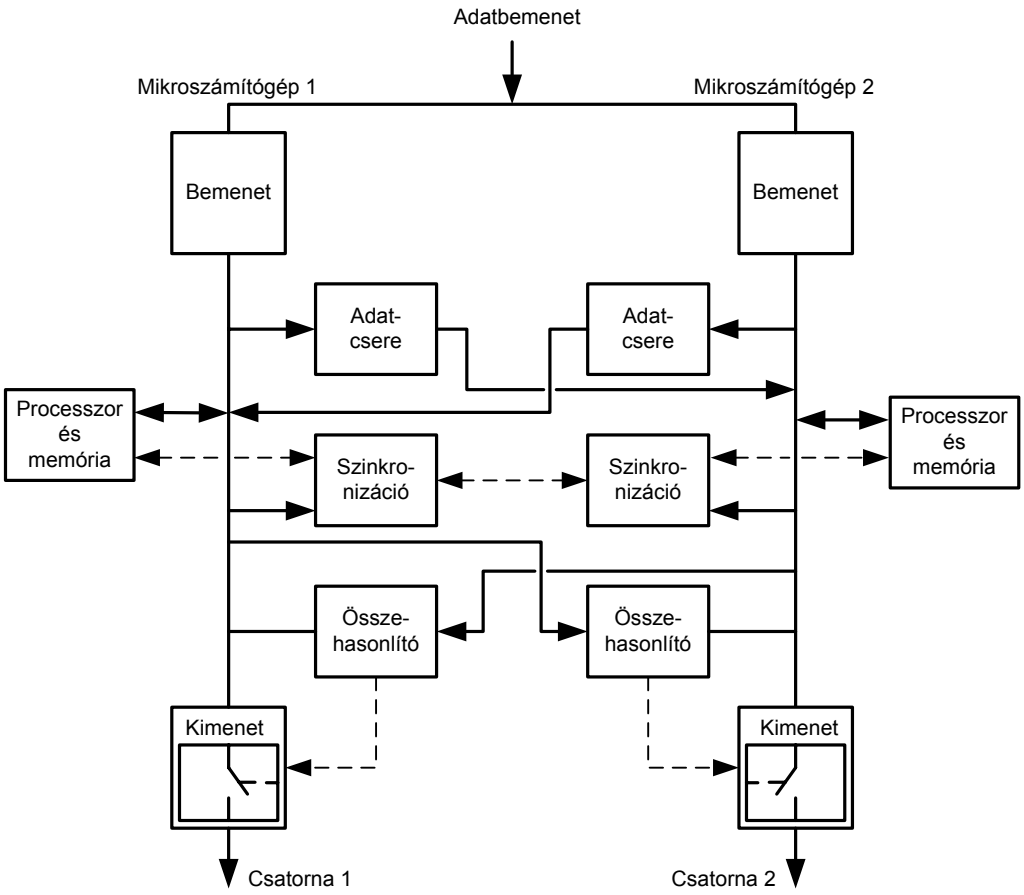
---



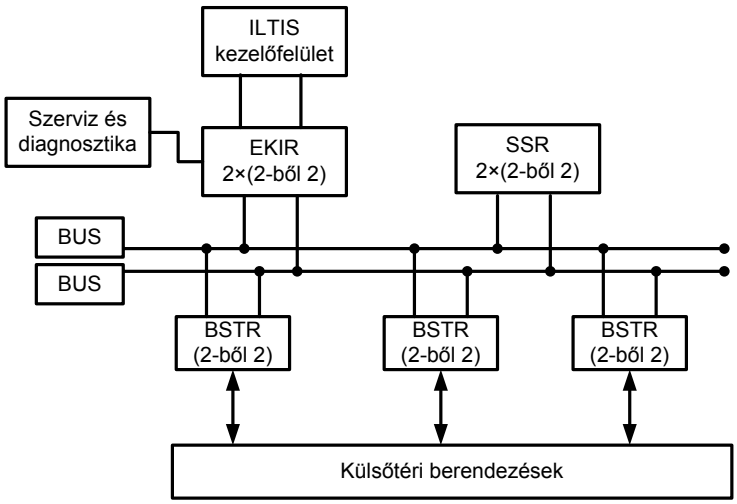
1. ábra A 2-ből 2 elv



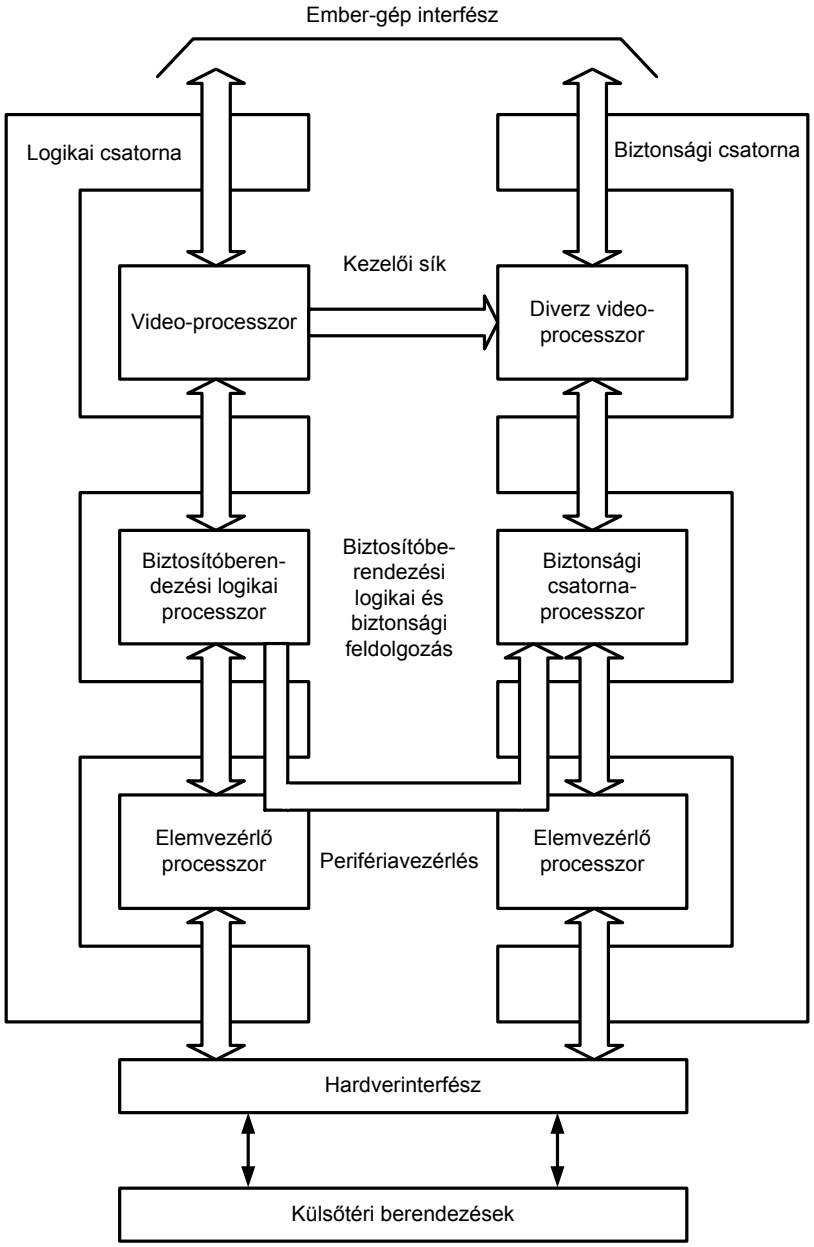
2. ábra A 3-ból 2 elv



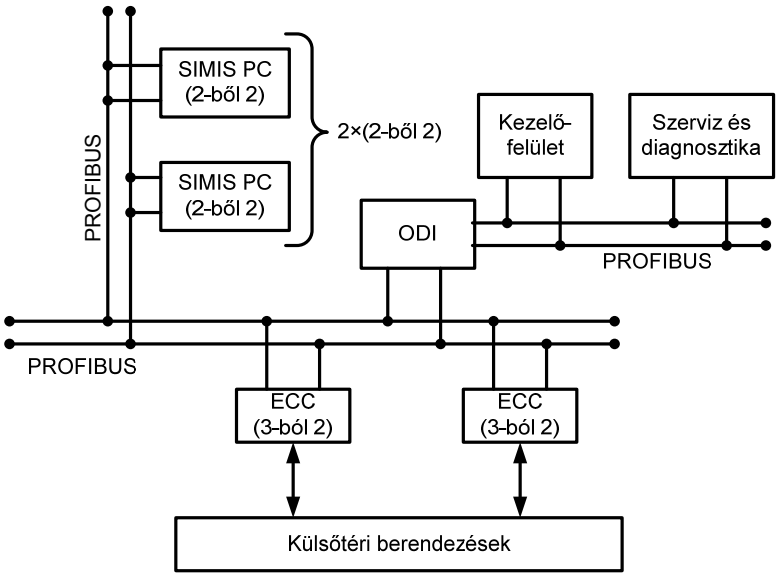
3. ábra A SIMIS elv



4. ábra A tatai berendezés felépítése (SIMIS C)



5. ábra Az ELEKTRA rendszer



6. ábra A SIMIS IS rendszer