Automatika - Közlekedésautomatika 5.

Logisztikai mérnök MSc szak
Közlekedési mérnök MSc szak

Biztonsági rendszerek

Biztonsági rendszerek helye az irányítástechnikai megoldások között

- Az irányítás alapvető megoldási lehetőségei
  - vezérlés,
  - szabályozás.
- A biztonsági rendszerek speciális irányítástechnikai megoldása a biztonsági kör
- Biztonsági kör helye a vezérlés-szabályozás megoldásai között

A vezérlés alapvető jellemzői (1)

- Cél: meghatározott állapotjellemzők (üzemi paraméterek) célirányos befolyásolása
- Feladat: beavatkozás az irányítandó folyamatba, meghatározott beavatkozó szervek (ún. aktorok) segítségével. (lehetséges aktorok pl. szelep, állító ellenállás, adagoló szivattyú, léptető motor, stb.)

A vezérlés alapvető jellemzői (2)

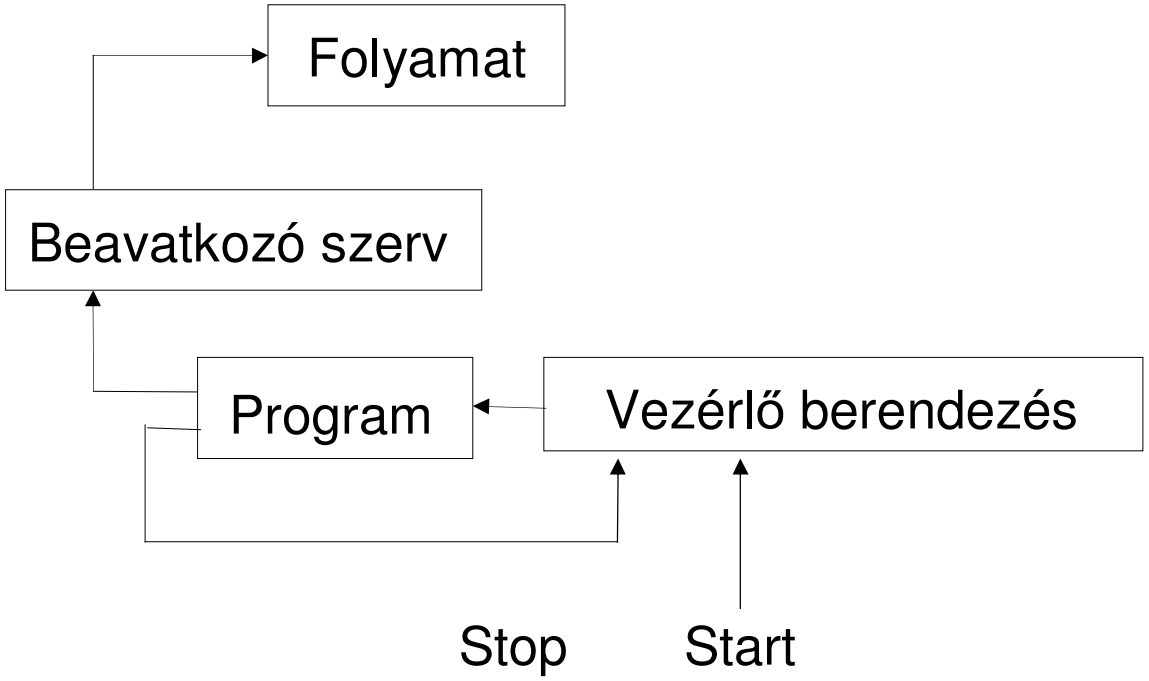
- Jellemző: A vezérlés hatáslánca nyitott - a jelek átvitele csak egy irányban történik (alapvetően ez különbözteti meg a zárt hatásláncú szabályozástól)
- A vezérlés különböző kialakítási lehetőségei
  - Programvezérlés
  - Ütemezett programvezérlés
  - Követő programvezérlés
  - Jelzésvezérlés

Programvezérlés (1)

- A kezelő személyzet rendszeresen ismétlődő tevékenységét automatizálja - különösen jól mutatja a nyitott hatásláncot
- A program a folyamat által meghatározott sorrendben parancsokkal működteti a beavatkozó szerveket
- Program az indító (start) parancs után egyszer vagy többször lefut - függetlenül a beavatkozás sikerétől

Programvezérlés (2)

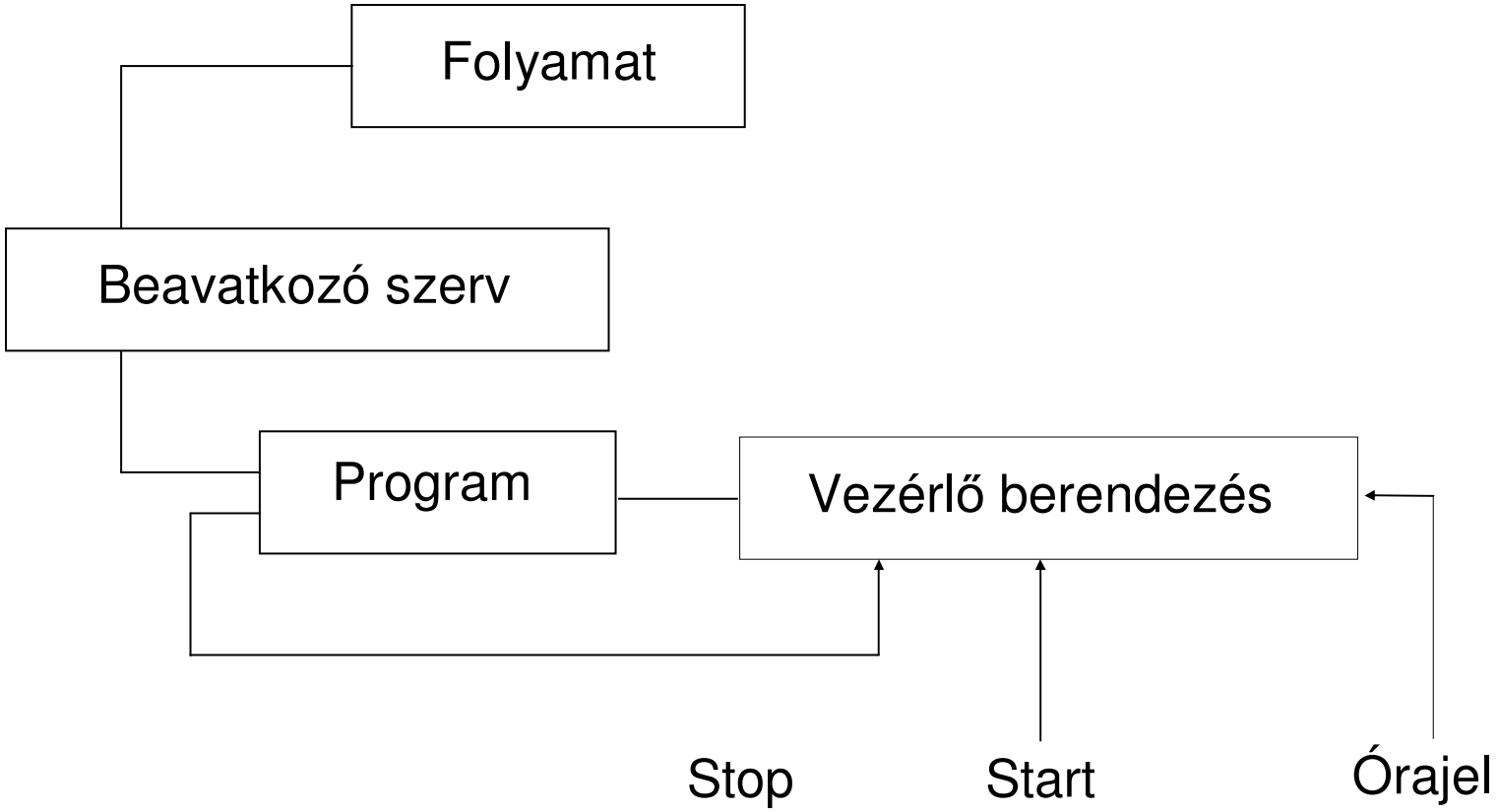
Minden programvezérlés esetén ismerni kell a vezérlésnek a folyamatra gyakorolt statikus és dinamikus hatását



Ütemezett programvezérlés (1)

- Ebben az esetben a lépéseket órajel vezérli
- Példa az ütemezett programvezérlésre a jelzőlámpás közúti forgalomirányítás, melynél a forgalom változásához a programok időnkénti váltásával lehet alkalmazkodni. (Ez még nem forgalom-szabályozás!)

Ütemezett programvezérlés (2)



Követő programvezérlés (1)

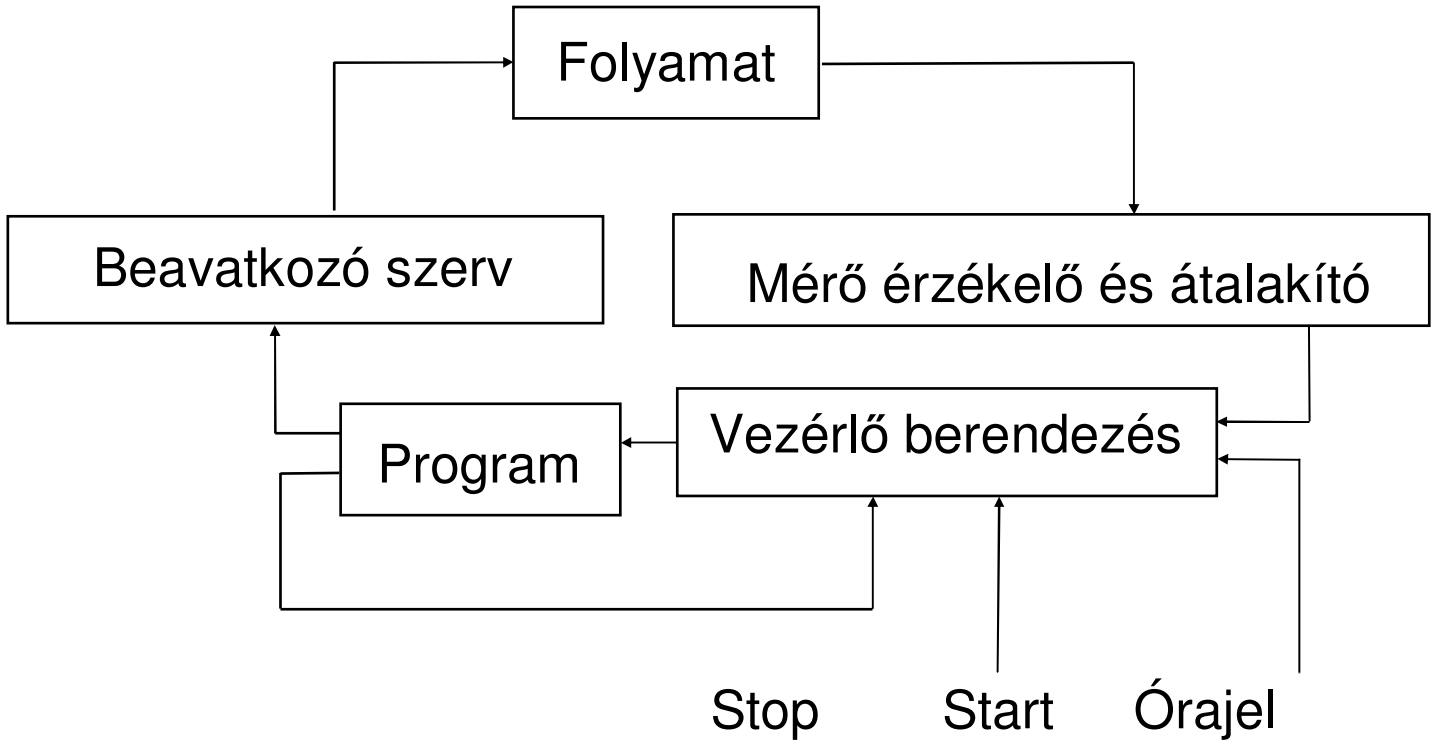
- A követő programvezérlés esetén a következő programlépés végrehajtásának előfeltétele az előző lépés eredményes befejezése
- A lépés befejezésének érzékelésére mérni kell a folyamat állapotjellemzőit, ebből kell működési határértékeket képezni.

Követő programvezérlés (2)

- Pl.1.: Jelzőlámpás forgalomirányító berendezés kiegészítve járműérzékelő szenzorokkal - ezzel a forgalom bizonyos hatást gyakorol a program lefutására
- Pl.2.: Automatikus telefonközpontok
- Pl.3.: Levélosztályozó automata
- Pl.4.: Ipari folyamatok indítása, leállítása, szakaszos üzemű gyártási folyamatok
- pl.5.: Vasúti forgalomirányító automatika - vasúti biztosítóberendezés

Követő programvezérlés (3)

Blokkvázlata a következő:



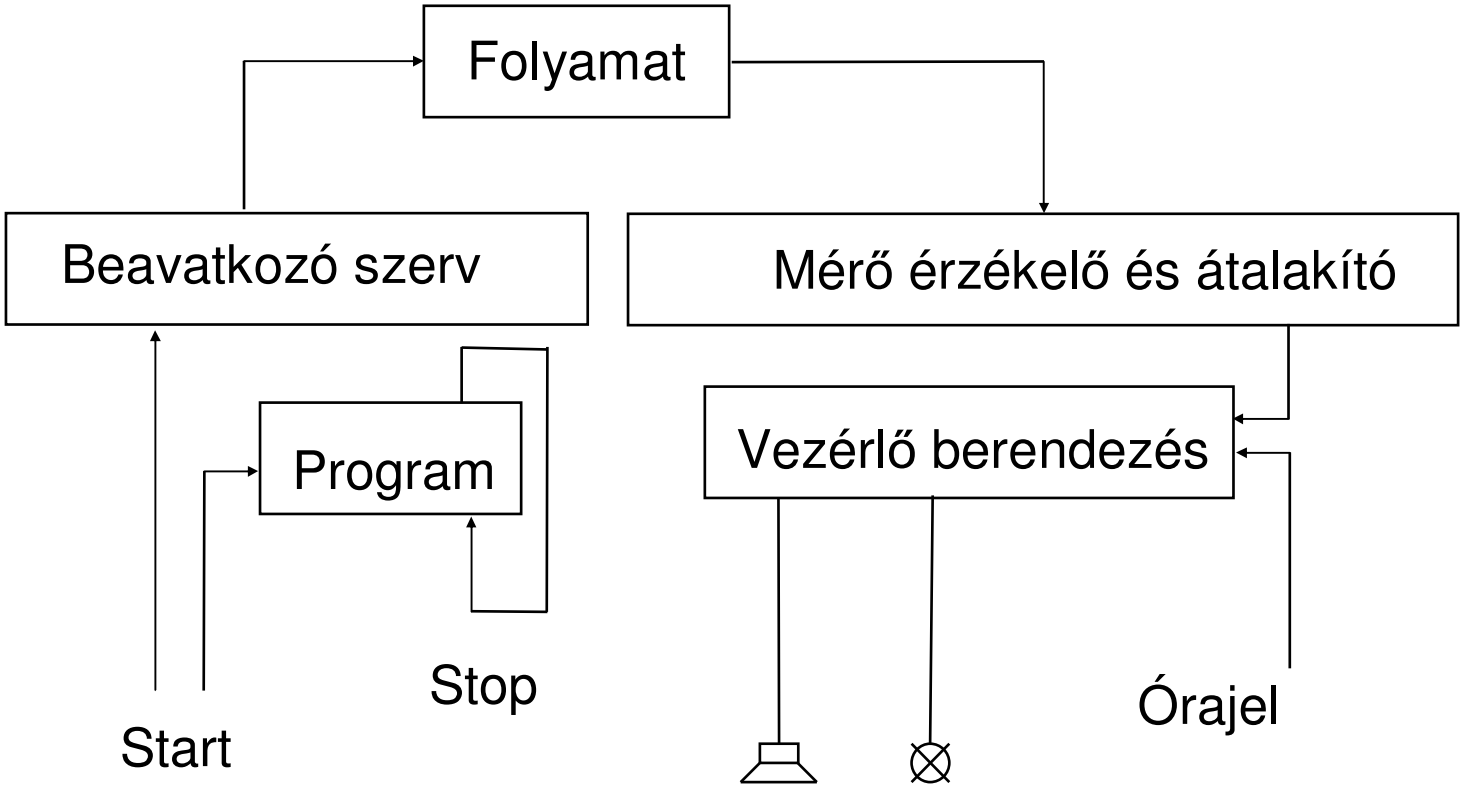
Követő programvezérlés (4)

- Hatáslánc $\Rightarrow$ spirálszerűen emelkedő (nem zárt)
- A mért határérték és az órajel együtt gondoskodik a program késleltetett vagy ismételt újraindításáról

Követő programvezérlés (4)

- Az ábra alapján téves lenne a „szabályozó kör” elnevezés - itt még nincs zárt kör, csupán „vezérlő spirál” („~ lánc”): minden ütem után a folyamat egy következő, magasabb programsíkra kerül.
- A vezérlés lényeges jellemzője: a folyamatra gyakorolt hatás nem hat vissza magára a vezérlésre

Jelzésvezérlés (1)



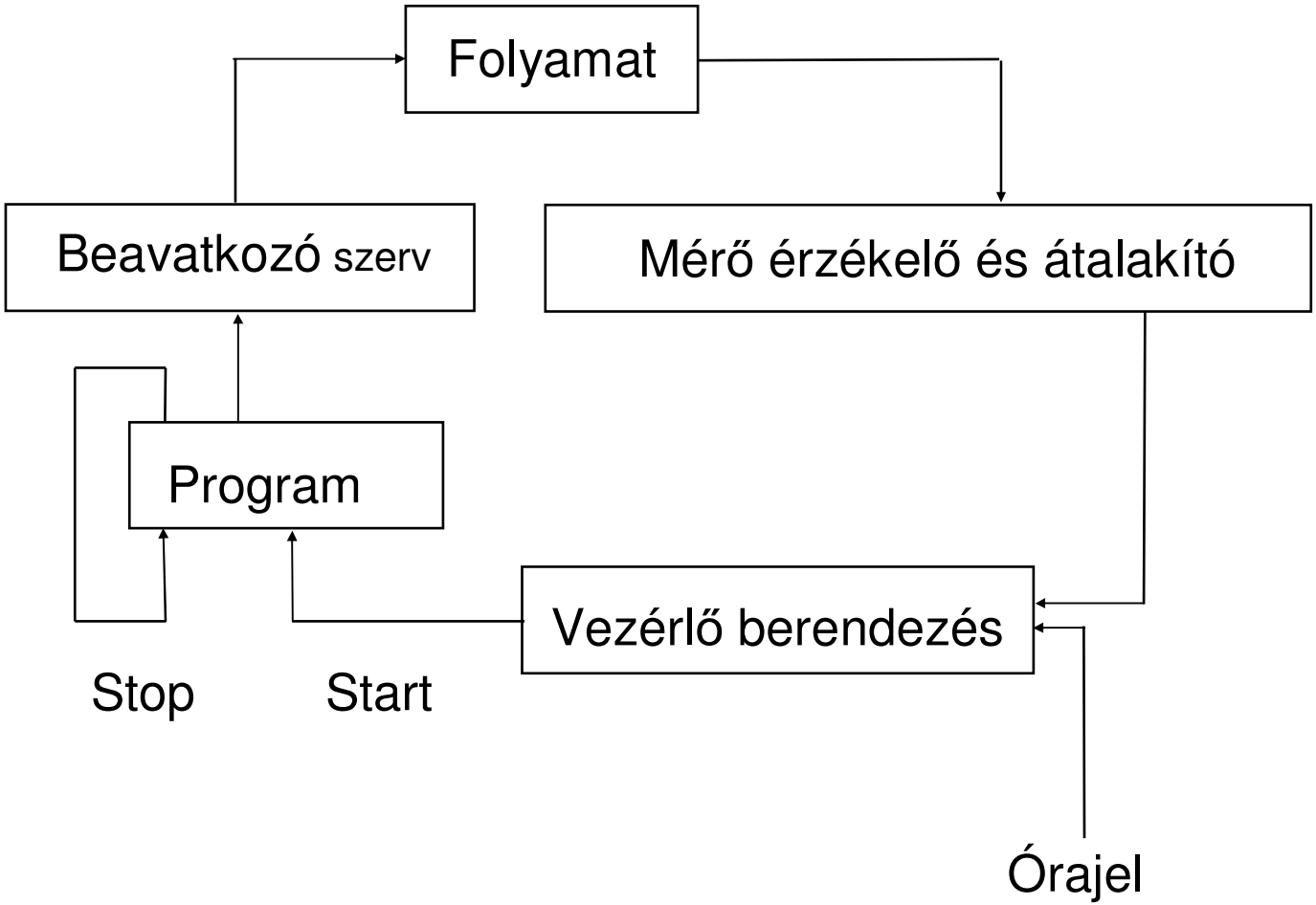
Jelzésvezérlés (2)

- A jelzésvezérlés esetén elmarad a készülékszintű kapcsolat a vezérlő berendezés és a program között
- A mért és képzett folyamat-határtékek más fizikai (pl. optikai, akusztikus) úton jelennek meg
- Ez a mérőberendezés automatikus leolvasásának felel meg

Jelzésvezérlés (3)

- A jelzés alapján kézi beavatkozás lehetséges (esetleg biztonsági intézkedések foganatosíthatók)
- Gyakori megoldás a különböző folyamatirányító rendszereknél

Biztonsági kör (1)

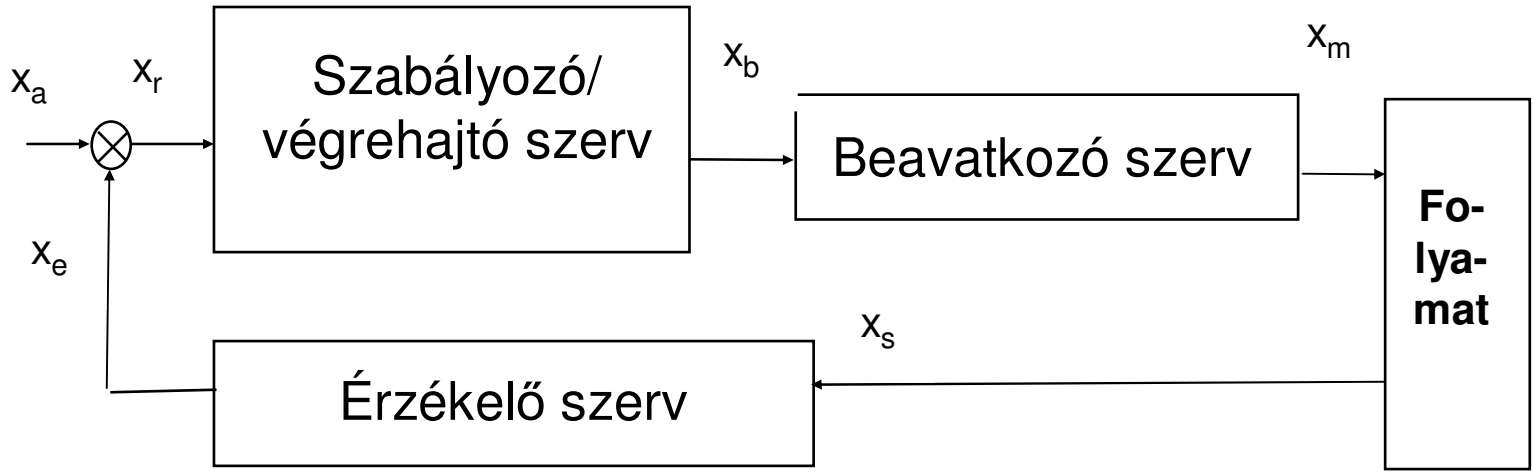


Biztonsági kör (2)

- A jelzésvezérlés speciális esete:
  a vezérlő berendezésben képzett jel a program bizonyos biztonsági szükség-intézkedésének egyszeri végrehajtását eredményezi
- Hatáslánc $\Rightarrow$ egyszeri spirál

Szabályozás (1)

- A szabályozás olyan eljárás, amellyel egy berendezés folyamatjellemzőjét (x_s) a beavatkozó jel (x_b) segítségével a zavaroktól (x_z zavaró jel) lehetőleg függetlenül meghatározott (állandó, vagy előírt módon változó) értéken tartjuk.



- xa - alap-jel (a szabályozási kör bemenő jele)
- xb - beavatkozó jel (végrehajtó szerv kimenő jele)
- xe - ellenőrző jel (érzékelő kimenő jele)
- xm - módosított jellemző (a rsz bemenő jele)
- xr - rendelkező jel (= xa - xe)
- xs - szabályozott jellemző (a rsz kimenő jele)
- xz - zavaró jel

A vezérlés, szabályozás és biztonsági kör kapcsolata (1)

- Az összehasonlítás alapja a folyamatba való beavatkozást elősegítő információk eredete és felhasználási módja:
  - A *vezérlés*sel az előre látható események tapasztalati értékek alapján kívánt módon befolyásolhatók (a „tapasztalat” itt a folyamat tulajdonságaiból adódó és a programban tárolt információkat jelenti);

A vezérlés, szabályozás és biztonsági kör kapcsolata (2)

- a *szabályozás* addig működik, amíg eltérés mutatkozik a kívánt állapottól: az ehhez szükséges információk a folyamat állandó megfigyeléséből származnak;
- a *biztonsági kör* valamely zavar esetén egyszeri ellenintézkedést foganatosít.

- Az összehasonlítás alapján a biztonsági kör fogalmilag a **vezérlés és szabályozás között** foglal helyet

A vezérlés, szabályozás és biztonsági kör kapcsolata (3)

- A szükséges információ a folyamatból származik (mint a szabályozásnál),
- az információ hatására történő beavatkozás előre programban rögzíthető (mint a vezérlés esetén),
- a programvezérléshez hasonlóan a rendszert ilyen zavar esetben (automatikusan vagy kezelői beavatkozásra) egy biztonságos állapotba viszi.

Biztonsági rendszerekkel szembeni alapvető követelmények

- Megfelelő műszaki kialakításon túl fontos, hogy a rendszer:
  - kezelése,
  - fenntartása
  - kifogástalan legyen.
- A rendszer kialakításának védeni kell a
  - véletlen és
  - szándékos hibák ellen, és a
  - kezelési hibák ellen.

Veszély megjelenése a műszaki rendszerekben

- hibás vezérlő jelek következtében (pl. hibás váltóállítás egy vasúti automatikában),
- ellenőrző rendszer kikapcsol(ód)ása miatt (valamely védőrendszer meghibásodása)

Biztonsági rendszerekkel szembeni követelmények

- A védelem **megbízható**an működjön
- A védelem **kényszerűen hatásos** legyen
- A védelem **megkerülhetetlen** legyen

A védelem megbízható működésének feltételei

- Egyértelmű működésmód
  - megfelelő konstrukció
  - megfelelő működési alapelvek
- Jól bevált elvek szerint kialakított elemek használata
- Ellenőrzött gyártás és szerelés
- Üzembehelyezés előtti próbák

A védelem kényszerű hatásosságának feltételei

- Veszélyes állapot kezdetétől annak teljes időtartama alatt jelen legyen
- Védőintézkedés feloldásakor a veszélyes állapot kényszerűen fejeződjön be
- Pl.: centrifuga lezárt fedéllel indítható, lift bezárt ajtókkal indul, stb.

A védelem megkerülhetetlenségének feltételei

- A reteszelő berendezés a rendszer szerves részét képezze – sem szándékosan, sem véletlenül ne legyen kiiktatható

Pl. Mozdonyok éberségi berendezése, a biztonsági menetkapcsoló (Si-Fa =Sicherheitsfahrschaltung)

A védőreakciók megvalósítási lehetőségei

- Visszajelentés alkalmazása
- Önellenőrzés alkalmazása
- Redundancia alkalmazása
- Bistabil elemek alkalmazása
- Újraindítás reteszelése
- A védő funkció vizsgálhatósága

Visszajelentés alkalmazása

- beavatkozás tényének, okának rögzítése
- beavatkozás módja a folyamat sebességétől függően
  - egyfokozatú - azonnali beavatkozás
  - kétfokozatú - először figyelmeztető jelzés, majd beavatkozás

Önellenőrzés alkalmazása

- Védelem bekapcsolása veszély esetén és meghibásodás esetén
- Önellenőrzés megvalósítása
  - nyugalmi áramú elv
  - munkaáramú elv - csak ellenőrző kapcsolás alkalmazása mellett

Redundancia alkalmazása (1)

- Térbeli redundancia (párhuzamos redundancia)
  - Forró tartalék - a tartalék elem teljes idő alatt teljes terheléssel működik
  - Meleg tartalék - a tartalék elem a meghibásodásig kisebb terheléssel működik
  - Hideg tartalék (Stand-by) - a tartalék elem a meghibásodásig nincs terhelés alatt

Redundancia alkalmazása (2)

- Időbeli redundancia (időszakos hibák, zavarok ellen): információ-feldolgozás időben egymásután (kétszeres -, többszörös feldolgozás)
- Elv-redundancia - a redundancia speciális megjelenési formája: az adott funkció ellátására alkalmazott tartalékegységek más-más elven működnek

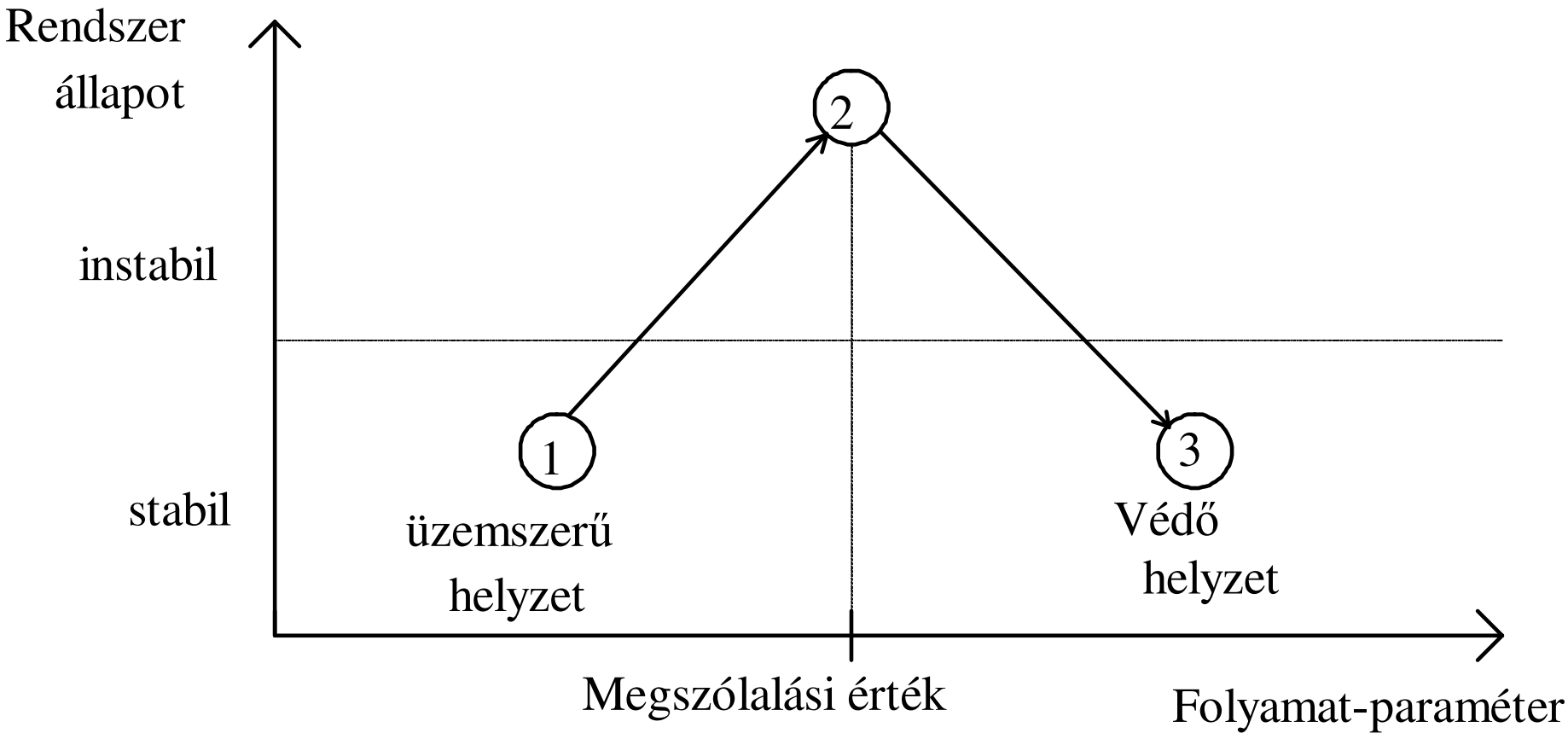
A redundancia bevezetésének szintjei

- alkatrész redundancia (többlet -, vagy speciális alkatrész) – pl. biztonsági jelfogó
- készülék redundancia – a megbízhatóság növelés szempontjából kedvezőbb megoldás,
- rendszer-redundancia

Bistabil elemek alkalmazása

- Védőrendszer működtetése meghatározott megszólalási értéknél (ezen érték alatt és felett stabil -, az értéknél pedig instabil állapotban van a rendszer)

Bistabil elem működésmódja



Újraindítás reteszelése

- Más elnevezés: „ismétlőzár” funkció
- Védőrendszer megszólalása után önműködően nem vihető ismét normál üzemi helyzetbe
- További üzem csak a kialakult helyzet ellenőrzése után lehetséges

Vizsgálhatóság

- Védőrendszer veszély helyzet nélkül is megszólaltatható legyen - veszélyhelyzet szimulációja!
- Vizsgálat módja
  - indítás vizsgálat (felfutás vizsgálat)
  - rendszeres vizsgálat

Az automatikák kialakításának gazdasági vonatkozása

- Biztonságkritikus rendszerek biztonsági szintjének meghatározásakor nem lehet gazdasági optimumra törekedni,
- Tökéletes biztonság nem érhető el, a rendelkezésre álló anyagi lehetőségek végesek
- Az elegendő biztonsági szint meghatározásához az élet alapkockázata jelentheti az objektív alapot

Az automatizálandó folyamat jellemzői (1)

- a folyamat **veszélyessége**: baleseti statisztikák alapján különböző ipari és közlekedési területekre (ún. veszély-potenciál sor, megítélése gyakran szubjektív!)

Az automatizálandó folyamat jellemzői (2)

- Veszélypotenciál sor – baleseti statisztikai adatok alapján rangsorolva közli a különböző biztonságkritikus rendszereket:
  - Háztartási berendezések
  - Gépi működtetésű kapuk
  - Nagyfeszültségű kapcsolók
  - Gépjármű
  - Orvosi készülékek
  - Emelő szerkezetek
  - Mozgólépcsők

- Veszélypotenciál sor (folytatás)
  - Tüzelő berendezések
  - Daruk
  - Drótkötélpálya
  - Közúti jelzőlámpák
  - Felvonók
  - gőzkazánok
  - Vasúti biztosítóberendezések
  - Olajfúró szigetek
  - Repülőgépek
  - Kémiai reaktorok
  - Atomreaktorok

  Stb. ….

Az automatizálandó folyamat jellemzői (3)

- a folyamatban lehetséges **biztonságos állapotok száma** – az üzemszerű állapot jól megtervezett rendszernél mindig biztonságos, fontos kérdés, hogy meghibásodás esetére **van-e biztonságos tartalékállapot?**
- az **ember szerepe** a folyamatban (ember elválasztható-e a veszélyforrástól?).

Biztonsági automatika rendszerek (1)

- A folyamat automatizálásának biztonságfilozófiáját alapvetően a folyamat fenti biztonsági jegyei határozzák meg.
- Ha a rendszernek nincs biztonságos tartalék-állapota (safe life technológia), akkor a meghibásodásokat nagy valószínűséggel ki kell zárni

Biztonsági automatika rendszerek (2)

- Ha a rendszernek van biztonságosan elérhető tartalékállapota (ún. fail-safe technológia), akkor a meghibásodás esetén törekedni kell e tartalék állapot elérésére

Biztonsági automatika rendszerek (3)

Az automatikák biztonságos kialakítását eldöntő kérdések:

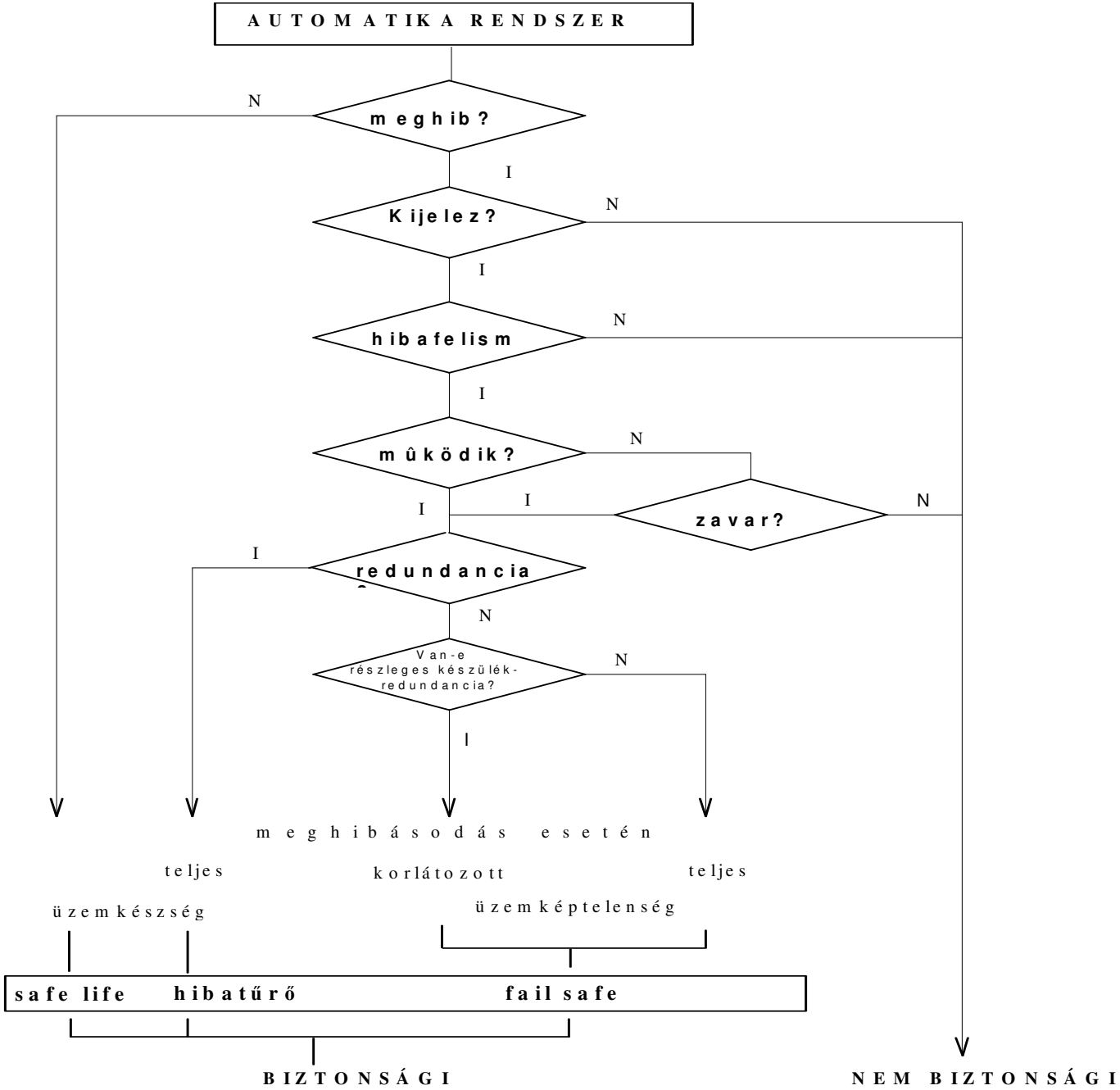
- Kell-e a rendszerelemek **meghibásodás**ával számolni?
- Hiba esetén van-e megfelelő **hibafelismerési mechanizmus** a hibák érzékelésére?
- Ha igen, az **kijelzi-e** a fellépett hibákat (azok legalább zavarként jelentkeznek-e?)
- Van-e a meghibásodok esetére **redundancia** a rendszerben?

Biztonsági automatika rendszerek (4)

- Fenti kérdésekre adott különböző válaszok alapján megkülönböztethető biztonsági automatika rendszerek:
  safe life, fault tolerant és a fail-safe rendszer!
- Definiciók:
  - **safe life** (=*„hibamentes”*) **rendszer** - az engedélyezett üzemidőn belül nem kell meghibásodással számolni (rendszeres felülvizsgálatot igényel),

Biztonsági automatika rendszerek (5)

- **fault tolerant** (=*„hibatűrő”*) **rendszer** - kell számolni meghibásodással, azt a hibafelismerő mechanizmus felismeri, vagy zavarként kijelzi, teljes készülék-redundancia meghibásodás esetére is teljes üzemkészséget garantál
- **fail safe** (=*„hibabiztos”*) **rendszer** - mint előbb, de nincs, vagy csak részleges készülék-redundancia van, emiatt meghibásodás esetén részleges vagy teljes üzemképtelenséggel kell számolni


AUTOMATIKA RENDSZER
meghib?
N
I
Kijelez?
N
I
hibafelism
N
I
mûködik?
N
I
I
zavar?
N
I
redundancia
N
Van-e részleges készülék-redundancia?
N
I
meghibásodás esetén
teljes
korlátozott
teljes
üzemkészség
üzemképtelenség
safe life
hibatűrő
fail safe
BIZTONSÁGI
NEM BIZTONSÁGI

Biztonsági rendszerek kialakítási módjai

Biztonsági rendszerek megvalósítási lehetőségei (1)

- A hibabiztos (valódi fail-safe) tulajdonság: a funkcióban jelentkező meghibásodások közvetlenül eredményezik a rendszer biztonságos állapotát. *Realizálási mód:* a vezérlő rendszerben az energia szegény (illetve energiamentes) állapotot reteszelés, tiltás értelmében használják.
- A jelfogós rendszerek általában fail-safe módon viselkednek.
- A biztonsági jelfogó konstrukciójánál fogva hibabiztos tulajdonságú - megfelelő kapcsolási elvek alkalmazásával teljesíthetők a biztonsági feltételek

Biztonsági rendszerek megvalósítási lehetőségei (2)

- A kvázi fail-safe tulajdonság: a meghibásodás nem közvetlenül vezet a biztonságos állapothoz, hanem egy ellenőrző kapcsolás kijelzi a hibát, és ezután kerül a rendszer a biztonságos állapotba.
  Realizálási mód: megfelelő biztonsággal rövid idő alatt működő ellenőrzés és lekapcsolás útján.
- NB.: az elektronikus, többcsatornás mikroprocesszoros rendszerek általában kvázi fail-safe módon működnek.

Biztonsági irányítórendszerek alapjai (1)

- Fail-safe elv
  - A (valódi) fail-safe tulajdonság: a funkcióban jelentkező meghibásodások közvetlenül eredményezik a rendszer biztonságos állapotát.
  - Realizálási mód: a vezérlő rendszerben az energia szegény (illetve energiamentes) állapotot reteszelés, tiltás értelmében használják.

Biztonsági irányítórendszerek alapjai (2)

- A jelfogós rendszerek általában fail-safe módon viselkednek – biztonsági jelfogók
  - N típusú (I. biztonsági osztály)
  - C típusú (II. biztonsági osztályú)
- A jelfogó konstrukciójánál fogva alkalmas fail-safe áramkörök kialakítására - megfelelő kapcsolási elvek alkalmazásával teljesíthetők a biztonsági feltételek

Biztonsági irányítórendszerek alapjai (3)

- Kvázi fail-safe elv
  - A kvázi fail-safe tulajdonság: a meghibásodás nem közvetlenül vezet a biztonságos állapothoz, hanem :
  - egy ellenőrző kapcsolás kijelzi a hibát, és ezután kerül a rendszer a biztonságos állapotba.

Biztonsági irányítórendszerek alapjai (4)

- Kvázi fail-safe elv realizálási módja: megfelelő biztonsággal rövid idő alatt működő ellenőrzés és lekapcsolás útján.
- Az elektronikus, többcsatornás mikroprocesszoros rendszerek általában kvázi fail-safe módon működnek.

Elektronikus biztosítóberendezések lehetséges kialakítási formái

- A hardver tervezés és kivitelezés során a hibabiztos tulajdonságot kell megcélozni
- A szoftver szerepe függ a biztonsági feladatok hardver és szoftver közötti megosztásának módjától

Architektúra típusok

<table>
<tr><td colspan="3">HW ⇓
SW ⇒</td><td>Egy</td><td>Több</td></tr>
<tr><td>Egy</td><td></td><td></td><td>1. típus</td><td>5. típus</td></tr>
<tr><td rowspan="3">Több</td><td rowspan="2">Azonos</td><td>Szoros csatolás</td><td>2. típus</td><td></td></tr>
<tr><td>Mérsékelt csatolás</td><td>3. típus</td><td></td></tr>
<tr><td>Eltérő</td><td>Laza csatolás</td><td colspan="2">4. típus</td></tr>
</table>

1. típusú architektúra

Jellemző felépítés:

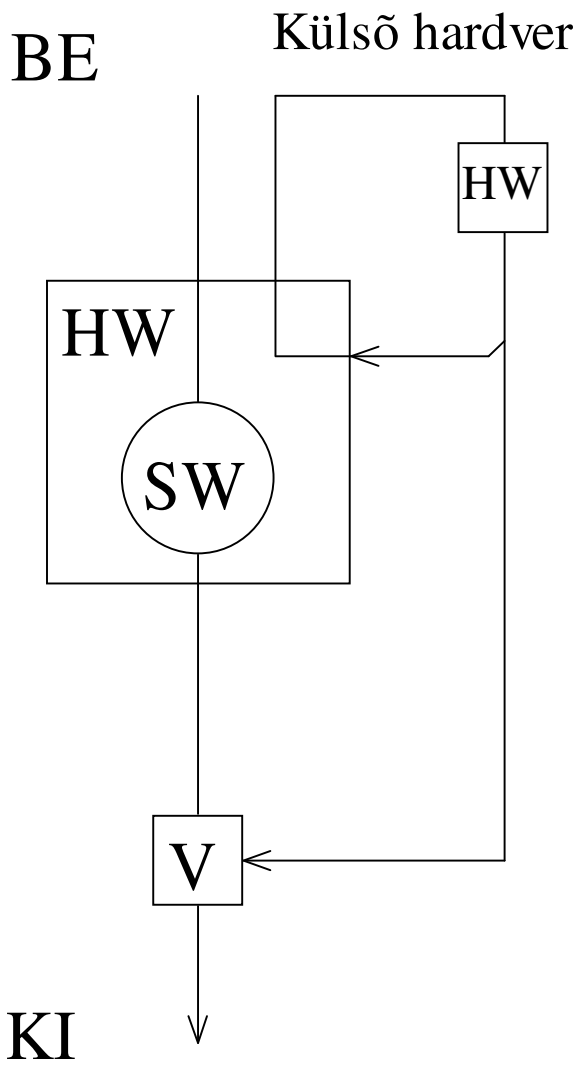
egy számítógép + egy program

Hibavizsgálat:

külső ellenőrző hardveren keresztül

Hardverhiba esetén:

rendszerkimenet meghatározott veszélytelen állapotba vihető



Az 1. architektúra típus értékelése (1)

- *Hardverhibák* felismerése az öndiagnosztikával rendelkező programoknál nehézkes (gyártó cég tesztjei hatékonyabbak)
- *Hardver meghibásodások* kijelzéséhez tesztprogramokat meghatározott maximális időn belül meg kell ismételni - ezzel a többszörös hibák valószínűsége korlátozható (Igen nehéz igazolni, hogy valamennyi meghibásodás-típus felismerhető-e?)

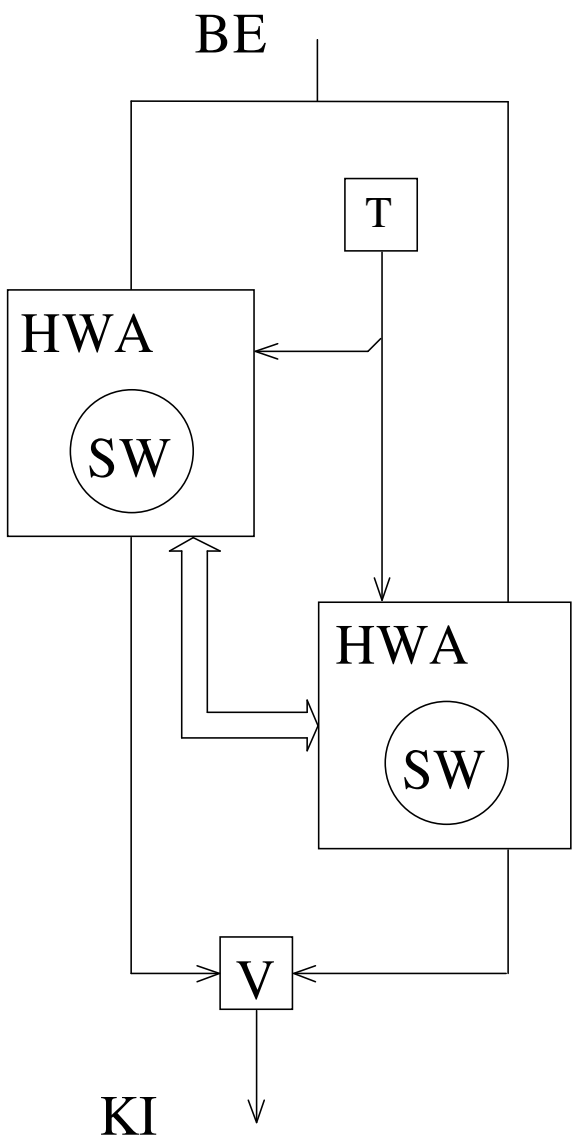
Az 1. architektúra típus értékelése (2)

- *Külső zavarok* felismerhetősége függ
  - a kontrollösszeg képzési módjától;
  - adatok aktualizálásának gyakoriságától,
  - hihetőségvizsgálat lehetőségeitől.
- *Szoftver-hibák* (program ill. adatok) felismerésére nem rendelkezik mechanizmussal, alapvető a szoftver hibamentessége!

Az 2. architektúra típus

Jellemző felépítés:
azonos számítógépeken azonos programok
(szorosan csatolt számítógépek)

Hibavizsgálat:
Számítógépek minden buszműveletét ellenőrizni egyezésre (közös órajel!)
A "V" összehasonlító csak egyezés esetén engedélyezi a biztonsági rendszerkimenetet



A 2. architektúra típus értékelése (1)

- *Hardverhibák*: megfelelő vizsgáló eljárásokkal kizárhatók (azonos gyártási hibák kizárása $\Rightarrow$ több gyártó, kellő minőségbiztosítás
- *Hardver-meghibásodások* közül
  - egyedül jelentkező meghibásodás nem kritikus,
  - független többszörös hibával rövid hibafelismerési idő esetén nem kell számolni,
  - azonos okra visszavezethető („common mode”) meghibásodásokra különös figyelmet kell fordítani

A 2. architektúra típus értékelése (2)

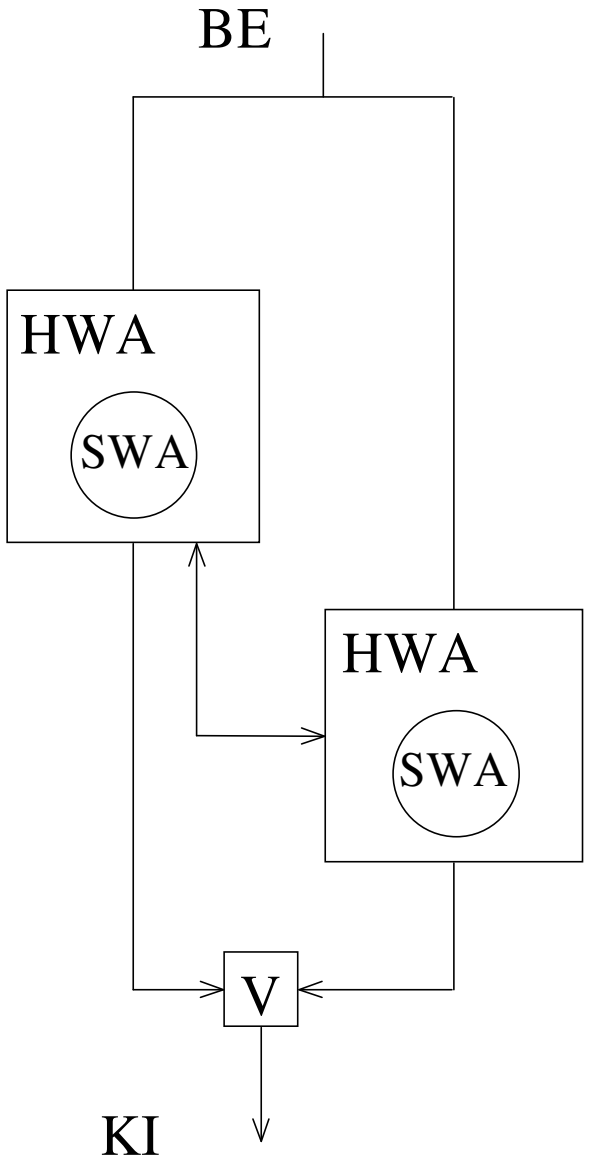
- *Külső zavarok* felismerhetősége hasonló, mint az 1. típusnál (tehát itt is kontrollösszeg, adatok aktualizálása ill. hihetőség vizsgálat szabja meg)
- *Szoftver-hibák* (program ill. adatok) felismerésére nem rendelkezik mechanizmussal, alapvető a szoftver hibamentessége!

A 3. architektúra típus

Jellemző felépítés: azonos számítógépeken azonos programok (mérsékelten csatolt számítógépek)

Hibavizsgálat:
tárolók és kimenetek állapotának kölcsönös ellenőrzése - összehasonlíthatóság érdekében
$\Rightarrow$ szinkronizáló jel!

Hiba esetén: számítógépek egymást kölcsönösen lekapcsolják



A 3. architektúra típus értékelése (1)

- Hardverhibák: több gépes rendszer lévén tervezési hibák kizárhatók;
- Hardver-meghibásodások:
  - meghibásodások különböző típusainak hatása hasonló a 2. típusnál mondottakra (egyszeres, független többszörös meghibásodás), de
  - meghibásodások felismerése csak a kimeneti-, vagy a tárolóállapot síkon lehetséges

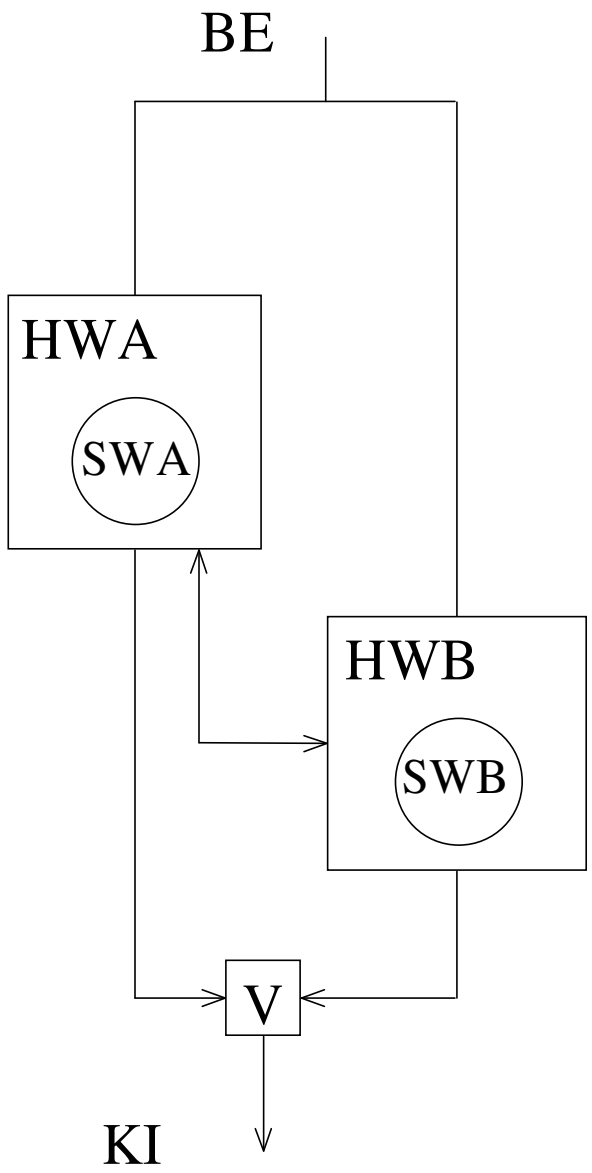
A 3. architektúra típus értékelése (2)

- *Külső zavarok* felismerhetősége hasonló, mint az 1. típusnál, a zavarok felismerhetőségét az aszinkronitás teszi egyszerűbbé
- *Szoftver-hibák* (program ill. adatok) felismerésére nem rendelkezik mechanizmussal, alapvető a szoftver hibamentessége!

A 4. architektúra típus

Jellemző felépítés:
(több lazán kapcsolt számítógép)
számítógépek és programjaik különbözőek lehetnek,
szinkronizáció igen laza

Lehetséges változat:
egyik gép végzi a számításokat,
másik ellenőrzi az eredményeket



A 4. architektúra típus értékelése (1)

- *Hardverhibák*: több gépes rendszer lévén tervezési hibák kizárhatók; különböző hardver-csatornák esetén azonos hatással jelentkező tervezési hibával nem kell számolni
- *Hardver-meghibásodások*: az egyszeres ill. a függetlenül jelentkező többszörös hibák hatása: mint a 2. típusnál (szoros csatolás!) a meghibásodások kijelzése ennél a típusnál a legnehezebb

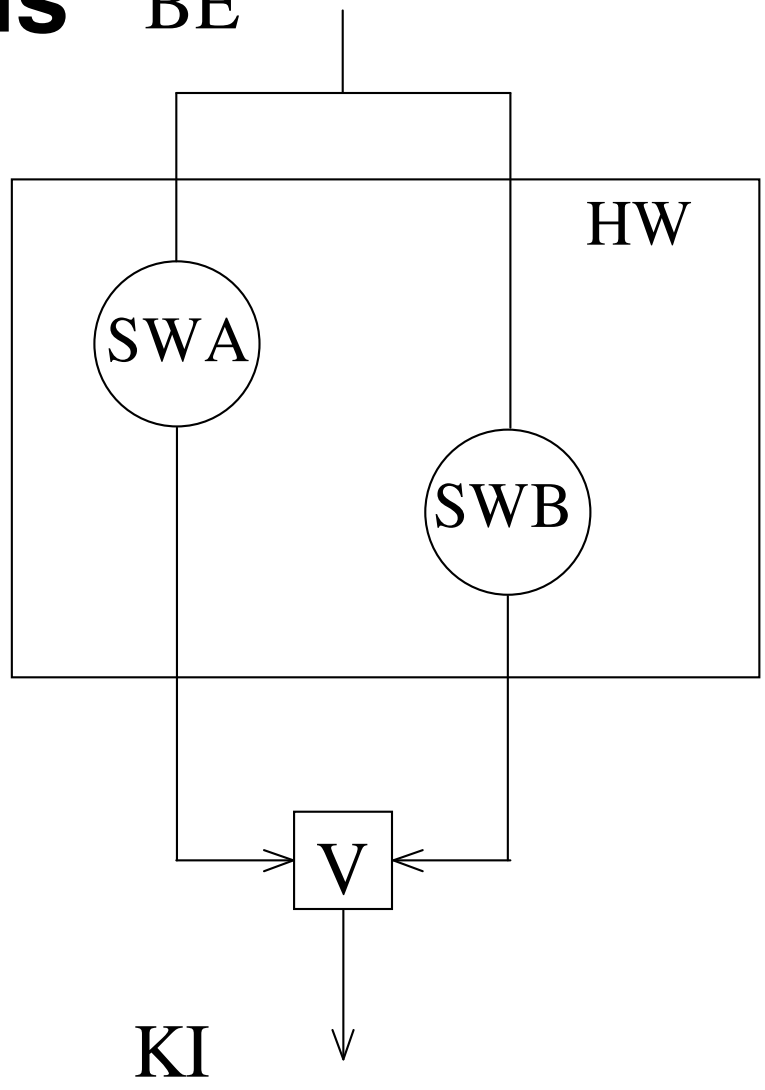
A 4. architektúra típus értékelése (2)

- *Külső zavarok* felismerhetősége hasonló, mint az 1. típusnál, a zavarok felismerhetőségét a diverzitás teszi egyszerűbbé
- *Szoftver-hibák* (program ill. adatok) szempontjából itt is fontos a szoftver hibamentessége, a hibák felismerését diverziter algoritmus ill. programozás segíti

Az 5. architektúra típus

Jellemző felépítés:
(egy számítógép két különböző programmal)

diverziter programok futása egy számítógépen ⇒ külső összehasonlító!



Az 5. architektúra típus értékelése (1)

- *Hardverhibák*: minden más úton ki nem zárható hiba felismerése e típusnál a szoftver feladata
- *Hardver-meghibásodások*:
  - független többszörös hibákkal rövid hibafelismerési idő esetén nem kell számolni
  - a „common mode” meghibásodások felismerhetősége függ
    - = a programok különbözőségének (diverzitás) mértékétől
    - = adatok aktualizálásának időközétől

Az 5. architektúra típus értékelése (2)

- *Külső zavarok* felismerhetősége hasonló, a zavarok felismerhetősége függ továbbá a program- és adat-diverzitás mértékétől
- *Szoftver-hibák* (program ill. adatok): itt is fontos a szoftver hibamentessége, hibafelismerés: diverzitás (algoritmus, programozás)

A biztonsági rendszerek kialakításának alapelvei (HW-1)

- Hardver moduláris kialakítása
  - Szekrényes építési mód
  - Keretes építési mód
- Szekrényes építési mód
  - számítógép-szekrények
  - interfész-szekrények
  - áramellátási szekrények
  - kábelszekrények

A biztonsági rendszerek kialakításának alapelvei (HW-2)

- Keretes építési mód (a nyomtatott áramköri lapokhoz)
- Nyomtatott áramkörös építési mód
  - a külsőtéri elemek nyomtatott áramköri lapjai
  - áramellátási összetevők nyomtatott áramköri lapjai
  - számítógépek nyomtatott áramköri lapjai
- Áramellátási egységek
- Kábelrendszer és csatlakoztatásai

A biztonsági rendszerek kialakításának alapelvei (SW-1)

- Szoftver moduláris kialakítása
  - a funkcionalitás jól áttekinthető egységekre osztása
  - felhasználói szoftver hierarchikus tervezése
  - magasszintű programnyelvek alkalmazása (strukturált programozás)
- Funkcionális egységek
  - bázis-szoftver (felhasználó-független)
  - felhasználói szoftver (adott felhasználó számára)
  - berendezés adatok (berendezés-függő)

A biztonsági rendszerek kialakításának alapelvei (SW-2)

- Felhasználói szoftver hierarchiája
  - rendszer
  - alrendszer
  - modul
- Programnyelvek választásának szempontjai
  - Gépi kódos
  - Assembly szintű nyelvek
  - Magas szintű nyelv
    - = Általános
    - = Célnyelv