Misák Sándor

PROGRAMOZHATÓ LOGIKAI VEZÉRLŐK

6. előadás

DE TTK

v.0.1 (2011.10.18.)

6. előadás

PLC-S VEZÉRLÉSEK MEGBIZHATÓSÁGÁNAK NÖVELÉSE

6. előadás

1. Üzembiztonsággal és megbízhatósággal kapcsolatos fogalmak;
2. TÜV ajánlások;
3. Az irányító rendszerek alkalmazásának biztonsági osztályai;
4. Biztonsági PLC-k rendszertechnikája;
5. Biztonsági PLC-k I/O konfigurációi.

ÜZEMBIZTONSÁGI ÉS MEGBIZHATÓSÁGI ALAPFOGALMAK

BEVEZETÉS, TÖRTÉNELEM

Napjainkban egyre inkább növekszik azon technológiai folyamatok száma, amelyek automatikus vezérlése fokozott biztonságot igényel.

Az energiaipar, vegyipar, közlekedés fokozott biztonsági követelményeket vet fel az élet és a vagyon megóvása érdekében.

Az automatikákat gyártó cégek különböző módszereket fejlesztettek ki, amelyekkel a berendezések üzembiztonsága javítható.

BEVEZETÉS, TÖRTÉNELEM

A módszerek mindegyike az irányító-berendezés valamilyen redundanciáján alapul.

A relés és diszkrét logikájú vezérlések idején a többségi logikákat (pl. 3-ból 2) alkalmazták a megbízhatóság növelésére.

Új igények és lehetőségek merültek fel a mikroprocesszoros berendezések, valamint a programozható logikai vezérlők megjelenése után.

BEVEZETÉS, TÖRTÉNELEM

Ezen készülékek sajátossága, hogy bár a központi egységük igen nagy megbízhatósággal működik, de ciklikus sorrendi és program szerinti működésük miatt egy esetleg fellépő zavar katasztrofális hibát okozhat.

A huzalozott logikához képest új hibaforrás a szoftverhiba.

BEVEZETÉS, TÖRTÉNELEM

Biztonságnövelő tényező, hogy az eszközök önmaguk tesztelésére is felhasználhatók, és a redundáns készülékek egymással kommunikációra képesek.

1980-ban jelent meg az első egymással kommunikáló redundáns PLC rendszer, 1981-ben a melegtartalék (hot standby) üzemmód, 1982-ben pedig az öntesztes PLC.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A mikroprocesszor alapú irányítóberendezések adatfeldolgozása valós idejű (real-time).

A valós idejű rendszer a fizikai folyamat lezajlásával közel azonos időben végzi el az információfeldolgozás és a beavatkozás feladatait.

Az üzembiztonság, ill. megbízhatóság növeléséhez elengedhetetlen a vonatkozó alapfogalmak, előírások és megoldások ismerete.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Elemnek valamely berendezés legkisebb alkotórészét nevezzük. Elem pl. egy integrált áramkör, ellenállás stb.

Modulnak egy berendezésben valamely feladat ellátására alkalmas, elemekből felépített, cserélhető egységet nevezzük. Egy számítógépben modul pl. valamely összetett funkcionális működést biztosító együttes (központi tár, központi feldolgozóegység stb.).

MEGBIZHATÓSÁGI ALAPFOGALMAK

Az elemet és a modult összefoglalóan részegységnek is nevezzük.

A rendszer bonyolult, összetett feladatok elvégzésére alkalmas berendezés, amely modulok kombinációjából áll.

A megbízhatóság a terméknek az a képessége, hogy az előírt funkciót elvégezze adott működési és környezeti feltételek mellett, miközben meghatározott tényleges működés alatt előírásos állapotban marad.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A megbízhatóság műszaki értelemben egy részegységnek (elem, modul) vagy rendszernek az a jellemzője, amely megadja, hogy az üzemeltetési feltételek fennállása esetén milyen mértékben várható el annak hibátlan rendeltetésszerű működése.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Matematikai értelemben a megbízhatóság statisztikai fogalom, amely annak a valószínűségét adja meg, hogy egy részegység vagy rendszer jellemzői az előírt határok közé esnek.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A megbízhatóság mennyiségi mutatóinak ismerete lehetővé teszi, hogy adott időpontban vagy időtartamban a berendezés hibátlan működésének vagy meghibásodásának valószínűségét meghatározzuk, a szükséges tartalékegységeket megtervezzük.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A számítógépes folyamatirányító rendszerek a megbízhatóság szempontjából veszélybiztos és működésbiztos rendszerekre oszthatók.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Ha a folyamat jellege olyan, hogy az irányítórendszerben bekövetkező egyedi hibák az élet- és vagyonbiztonság szempontjából veszélyes állapotot hozhatnak létre, a folyamat veszélybiztos irányítórendszert igényel.

A veszélybiztos irányítórendszer a hiba fellépésekor a folyamat leállításával képes a veszélyhelyzet kialakítását megakadályozni.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Ha a folyamat jellege olyan, hogy az irányítórendszerben bekövetkező egyedi hibák veszélyes állapotot nem hoznak létre, az irányítás működésbiztos rendszerrel megvalósítható.

A működésbiztos rendszer minden lehetséges hiba fellépésekor a folyamat csökkentett funkciójú működését biztosítja.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Ha a folyamat jellege olyan, hogy az irányítórendszerben bekövetkező egyedi hibák veszélyes állapotot nem hoznak létre, az irányítás működésbiztos rendszerrel megvalósítható.

A működésbiztos rendszer minden lehetséges hiba fellépésekor a folyamat csökkentett funkciójú működését biztosítja.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A redundancia valamely feladat elvégzéséhez feltétlenül szükséges eszközöket meghaladó számú, az eredetivel azonos funkciót ellátó eszközök (tartalékok) alkalmazása a megbízhatóság növelése céljából.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A redundancia egy rendszerben lehet gépi, információ- és programredundancia:

- **gépi redundancia esetén a berendezéseket többszörözik;**
- **információredundancia esetén az információhoz járulékos információt rendelnek (pl. paritásbit);**
- **programredundancia használatakor a programegységek többszörözésével növelik a megbízhatóságot.**

MEGBIZHATÓSÁGI ALAPFOGALMAK

A redundancia kialakítási szintjei:

Elemszintű redundanciával, pl. ellenállások vagy más áramköri elemek többszörösével, biztonságos áramkörök alakíthatók ki.

Elemszintű redundancia a programozásban pl. az utasítások ismétlése.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Modulszintű redundancia esetén a modulokon belüli alegységeket többszörözik.

Példa erre az olyan felépítésű analóg bemenet, amely két analóg/digitális átalakítót tartalmaz.

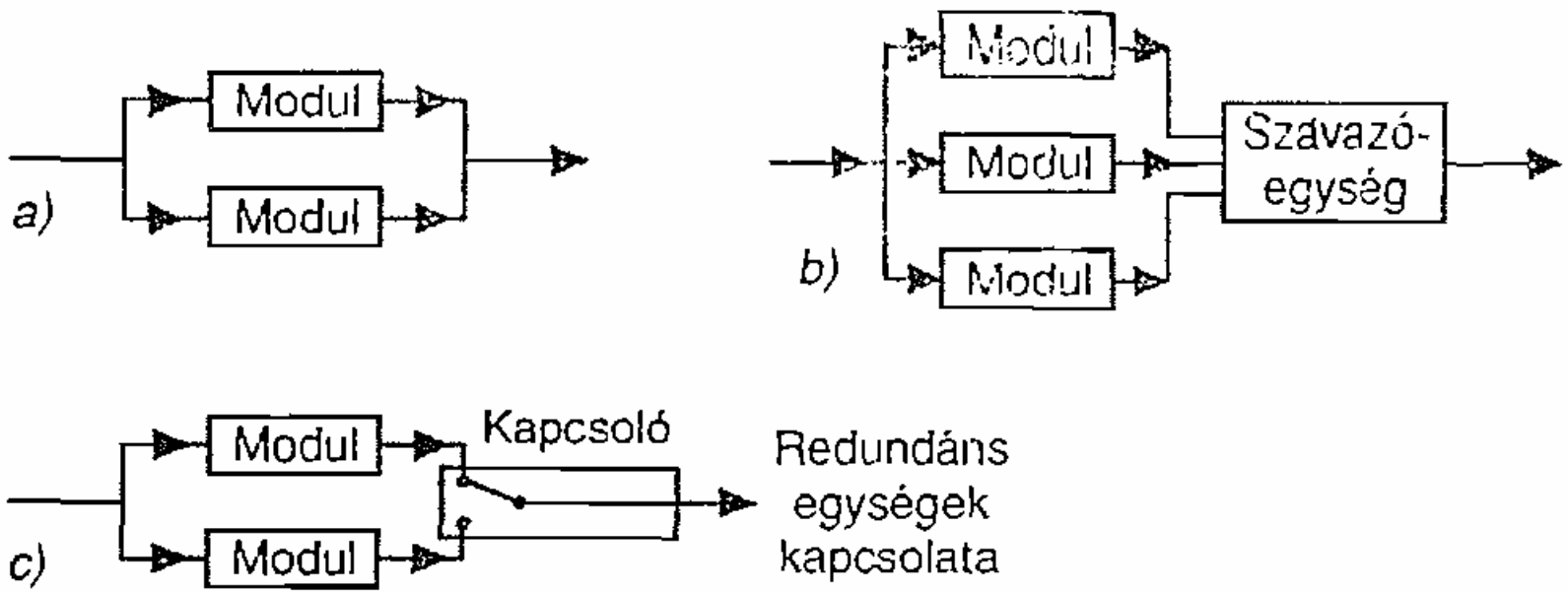
MEGBIZHATÓSÁGI ALAPFOGALMAK

Rendszerszintű redundancia esetén átkapcsolható vagy párhuzamosan működő modulokat alkalmaznak.

Program vonatkozásában a rendszerszintű redundancia a programmodulok többszörözését jelenti.

A redundáns egységek kapcsolata lehet párhuzamos, többségi (szavazó), ill. átkapcsolható.

MEGBIZHATÓSÁGI ALAPFOGALMAK



Párhuzamos (a), többségi (b), átkapcsolható (c) redundáns struktúra

MEGBIZHATÓSÁGI ALAPFOGALMAK

Párhuzamos redundancia esetén az egységek egy időben működnek.

A megbízható működéshez elegendő egyetlen egység működése.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A többségi elven működő redundáns egységek egy időben működnek, de kimenőjeleik a szavazóegységbe kerülnek.

A szavazóegység a bemenetére érkező információt kiértékelve a többségi elv alapján képezi a kimenő információt.

E megoldás esetén a szavazóegység azt az információt adja ki a kimenetén, amely legalább két modulnál megegyezik.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Átkapcsolható redundáns egységek esetén az egyik modul meghibásodásakor a kapcsoló átkapcsolja a rendszer kimenetét a hibás egységről a tartalék (stand-by) egységre.

A redundáns egységek alkalmazásának előnye a megbízhatóság növelése és az, hogy hibamentes esetben a tartalékegység járulékos irányítási feladatokat, vagy az irányítástól független feladatokat.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Hiba esetén egy rendszer működése az üzemi feltételek betartása mellett a megkívánt működéstől eltér.

Meghibásodás lép fel, ha egy elem vagy modul paraméterei üzemi feltételek mellett a specifikált határon kívül esnek.

A meghibásodás és a hiba definíciójából következik, hogy nem minden meghibásodás okoz hibát a rendszerben.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A két fogalom ismerete alapján belátható, hogy az üzem közben végzett rendszeres teszteknek milyen nagy a jelentősége.

A tesztekkel ui. a meghibásodások felfedhetők, mielőtt működési hibát okoznának.

A megbízhatóság elméleti vizsgálatához valószínűség-számítási és matematikai statisztikai módszerek szükségesek.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Az összefüggések és becslések megadásánál ún. javítható termékeket tételezünk fel.

Ez azt jelenti, hogy hiba esetén az adott részegységeket felújítják úgy, hogy a hiba megszüntetése után a részegység és a rendszer eredeti tulajdonságai teljesen helyreállnak.

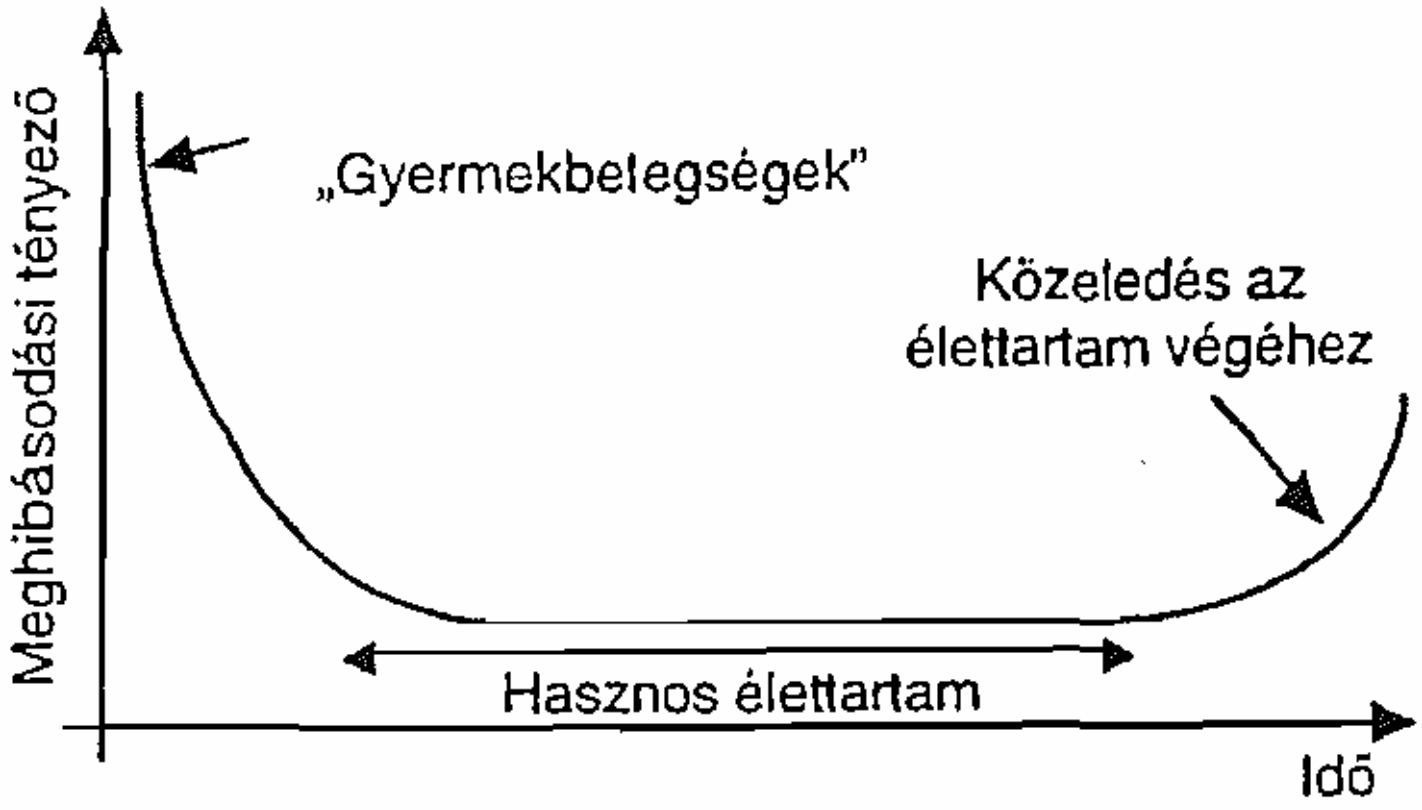
A javítható termékeket a H(t) helyreállítási függvénnyel jellemzik.

MEGBIZHATÓSÁGI ALAPFOGALMAK

E függvény megadja a javítható termék valamely kezdeti időpontjától számított, *t* időtartamú tényleges működése alatt bekövetkező meghibásodásainak várható értékét.

A meghibásodási tényező megadja, hogy adott időpont után, kis időegységen belül mekkora a meghibásodás valószínűsége, feltéve, hogy az adott időpontig a termék nem hibásodott meg.

MEGBIZHATÓSÁGI ALAPFOGALMAK



A termékek meghibásodási görbéje

MEGBIZHATÓSÁGI ALAPFOGALMAK

Egy termék meghibásodási tényezője az idő függvényében három szakaszra osztható.

A kezdeti időszakra a meghibásodási tényező fokozatos csökkenése jellemző. Ebben az időtartományban a hibák oka többnyire a gyártásra vezethető vissza.

A hasznos élettartamban a meghibásodási tényező gyakorlatilag állandó, véletlen hibák léphetnek fel.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Az elöregedési időszakban a meghibásodási tényező ismét növekszik, a termék minősége irreverzibilis változások miatt romlik.

Megfelelően gyártott és ellenőrzött gyártmányokra a meghibásodási tényező időfüggvényét megvizsgálva azt tapasztaljuk, hogy a kezdeti időszak igen rövid, a hasznos élettartam hosszú, így jó közelítéssel feltételezhető, hogy a meghibásodási tényező állandó.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A modulok meghibásodási tényezőinek ismeretében egy rendszer meghibásodási tényezője meghatározható.

A modulok megbízhatósági jellemzői az elemek megbízhatósági mutatói szerint számíthatóak ki.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A meghibásodások közötti átlagos működési idő (MTBF, Mean Time Between Failures) a folyamatirányító rendszerek megbízhatóságát jellemző mennyiségi mutató a két, egymást követő meghibásodás közötti hibátlan működés átlagos ideje.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A hibamentes működés valószínűségén annak valószínűségét értjük, hogy adott időszakaszban, előírt működési és környezeti feltételek mellett nem következik be meghibásodás.

Az átlagos helyreállítási idő (MTTR, Mean Time To Repair) a hibák behatárolására és megszüntetésére fordított kényszerű leállások átlagos ideje.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A PLC-k üzemvitelének jellemzői:

- **MTBF a meghibásodások közötti átlagos idő;**
- **MTTF a hibakiesésre jutó átlagos idő (Mean Time To Failure);**
- **MTTR a javításra fordított átlagos idő.**

MEGBIZHATÓSÁGI ALAPFOGALMAK

A PLC-k üzemideje:

$$\frac{MTBF}{MTBF + MTTR + MT},$$

képlet szerint jellemezhető százalékos értékben, ahol MT (Maintenance Time) a rendszeres karbantartási időt jelenti.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A λ átlagos hibaarány a:

$$\lambda = \frac{1}{MTBF},$$

képlet szerint határozható meg.

MEGBIZHATÓSÁGI ALAPFOGALMAK

λ bevezetésével a hibamentes várható élettartam:

$$R = \exp(-\lambda t).$$

Ha pl. egy PLC MTBF értéke 17500 óra (~2 év), akkor annak a valószínűsége, hogy a PLC egy évig (8750 óra) hibamentesen fog üzemelni:

$$R = \exp\left(-\frac{8750}{17500}\right) \approx 0{,}6.$$

MEGBIZHATÓSÁGI ALAPFOGALMAK

Az üzemi készenléti tényező annak valószínűsége, hogy a termék valamilyen *t* időpontban működőképes lesz.

Az üzemi készenléti tényező a termék rendelkezésre állását jellemzi, amely a meghibásodások közötti átlagos idő és az átlagos helyreállítási idő ismeretében meghatározható.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Az üzemi készenléti tényező a termék üzemeltetési adatai alapján:

$$K_k = \frac{teljes\_mukodesi\_ido \; - \; hiba\_miatti\_leallas\_idotartama}{teljes\_mukodesi\_ido} \cdot 100\%.$$

MEGBIZHATÓSÁGI ALAPFOGALMAK

A megbízhatósági mutatók egyikének vagy másikának megadása önmagában csak hiányosan jellemzi a megbízhatóságot, ezért célszerű egyszerre több megbízhatósági mutatót megadni (pl. az üzemi készenléti tényezőt és a meghibásodások közötti átlagos működési időt).

MEGBIZHATÓSÁGI ALAPFOGALMAK

A real-time folyamatirányító rendszerek létesítésekor a megbízhatósági követelmények figyelembevétele a tervezés legkorábbi fázisait is befolyásolja, ezért csak a megbízhatósági igények részletes felmérése alapján állítható össze egy folyamatirányító rendszer konfigurációja.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Az irányítási cél elérése szempontjából a lehető legnagyobb rendelkezésre állás biztosítása lenne a legkedvezőbb.

Az igényeket meghaladó megbízhatóság azonban felesleges többletköltségekkel jár, ezért műszaki és gazdasági okokból is fontos annak vizsgálata, hogy a kívánt irányítási cél biztosítása mellett egy folyamatirányító rendszerben milyen működéskíesés engedhető meg.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A megbízhatósági követelmények lehetnek:

- **leállás egyáltalán nem engedhető meg ;**
- **hosszú idejű leállás nem engedhető meg ;**
- **csak az adatbázis védelmét kell biztosítani.**

MEGBIZHATÓSÁGI ALAPFOGALMAK

Az első jelenti a legszigorúbb megbízhatósági követelményt.

Ez esetben működés közben semmilyen leállás nem következhet be, mert bármilyen hiba, amely működéskiesést okoz, katasztrofális hatású.

Az enyhébb megbízhatósági igény esetében a működésben csak hosszabb idejű leállások nem engedhetők meg.

A leállás idejét a technológiai folyamat időviszonyához kell hasonlítani.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Az ipari folyamatirányító rendszerek nagy része az enyhébb megbízhatósági kategóriához tartozik.

Ilyen rendszerek esetében általában kevésbé igényes mutató a két meghibásodás között eltelt idő, viszont a megbízhatóságot jól jellemzi az átlagos javítási idő, mivel ez adja meg a leállások várható átlagos időtartamát.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Az irányítórendszerek kis része tartozik a harmadik követelményhez, ahol a működéskiesés nem okoz nagyobb problémát, a gyakori, esetleg hosszabb idejű leállások megengedettek.

Ha egy leállást követő újraindításkor a meghibásodás előtti érvényes adatokból akarunk kiindulni, a teljes adatbázist valamely módon rögzíteni kell.

A leállás és javítás során biztosítani kell a védelmet.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A felsorolt megbízhatósági igények különböző rendszertechnikai megoldásokkal elégíthetők ki.

Az irányítórendszer megbízhatósági követelményeit befolyásoló tényezők a irányítandó folyamat technológiai sajátosságainak figyelembevételével:

- **a technológiai folyamat jellege;**
- **a technológiai folyamat állapotváltozásainak időviszonyai;**
- **a hiba kihatása a technológiai folyamatra.**

MEGBIZHATÓSÁGI ALAPFOGALMAK

A szakaszos üzemű folyamat irányítása során más megbízhatósági igények merülnek fel, mint a folyamatos technológiánál, mivel a folyamat továbbvitele többnyire kézi irányítással is biztosítható, ill. a folyamat akár hosszabb ideig is biztonságos állapotban tartható.

A technológiai folyamat állapotváltozá-sainak időviszonyai és a megbízhatósági igények között szoros kapcsolat van.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A technológiai folyamatok osztályai a bennük végbemenő állapotváltozások időbeli lefolyása alapján:

- **lassú folyamatok;**
- **gyors folyamatok.**

MEGBIZHATÓSÁGI ALAPFOGALMAK

Lassú folyamat esetén az állapotváltozási időértékek perc nagyságrendűek vagy nagyobbak, elegendő idő van a hibás beavatkozás korrigálására.

A kezelő közreműködésével a hibás berendezés megtalálható és kicserélhető, ill. a folyamat kézi üzemben is tovább működtethető.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Gyors folyamatok esetén az időértékek a perc, ill. másodperc tört részei, egy hibás beavatkozás rövid idő alatt kritikus helyzetet teremthet, ezért ennek megakadályozása itt különösen fontos.

A hibaészlelést, behatárolását és a hibás egység kiiktatását, ill. pótlását a folyamatirányítási üzem közben lehetőleg automatikusan kell végrehajtani.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Kézi vezérlés nem megengedett.

Az irányítási rendszer hibás működése anyagi eszközöket és embereket veszélyeztethet.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Az olyan rendszerekben, amelyekben a technológiai folyamatok sorosak és az egyes berendezések nagy gyártási kapacitásúak, az anyagi kár nagy lehet.

Egy berendezés helytelen üzemeltetése nagy mennyiségű hibás terméket hoz létre, és a többi sorosan működő berendezésre is hat.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Kevésbé szigorúak az irányítási rendszer megbízhatósági követelményei azokban a technológiai folyamatokban, amelyekben a gyártás párhuzamos. Az egyes ágak kiesése nem okozza a teljes rendszer leállását.

A számítógép üzemzavarakor, meghibásodásakor működésbe lépő berendezéseket háttérberendezésnek nevezzük.

A gyakorlatban a két számítógépes redundáns rendszerek a legelterjedtebbek.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Ha a rendszerben nincs meghibásodás, akkor az un. irányító számítógép végzi a folyamatirányítási feladatokat.

Meghibásodáskor a tartalék számítógép veszi át a folyamatirányítási funkciókat.

Átkapcsolható tartalék rendszer esetén a tartalék számítógép nem működik, ha nincs meghibásodás vagy legfeljebb azok a programok futnak a gépben, amelyek az átkapcsoláshoz szükséges információk felújítását végzik.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A tartalék számítógép ún. hideg- vagy melegtartalék lehet.

Hidegtartalék esetén az irányító számítógép meghibásodásakor a tartalék számítógépre való átkapcsolással egyidejűleg a tartalék számítógépet indítási állapotba kell hozni: programokat kell betölteni, a folyamatokat kell frissíteni stb.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Melegtartalék esetén a tartalék számítógép minden időpillanatban kész áttérni az alapműködésre.

A legtöbb folyamatirányítási feladatnál a tartalék számítógépre való átkapcsolást néhány másodperc alatt végre lehet hajtani és a funkciók zavartalanul folytathatóak, ezért melegtartalékos rendszert célszerű kialakítani.

Ez csak úgy valósítható meg, ha a tartalék és az irányító számítógépben futó programok állapota, az aktuális adatok induláskor azonosak.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Párhuzamos működésű tartalékrendszer esetén a tartalék számítógép az irányító számítógéppel egyidejűleg működik.

Csoportosításuk:

- **a párhuzamos működésű, azonos funkciójú tartalék rendszer (E kialakításban az irányító és a tartalék számítógépben gyakorlatilag egyidejűleg ugyanazok a programok futnak. Szinkronizáció szükséges.);**
- **a párhuzamos működésű, eltérő funkciójú tartalék rendszer (Ennek lényege, hogy a tartalék rendszer az irányító számítógéppel egyidejűleg működik, de attól eltérő feladatokat old meg.).**

MEGBIZHATÓSÁGI ALAPFOGALMAK

A párhuzamos működésű, eltérő funkciójú tartalék rendszer lehetséges kialakítá-sa az ún. alárendelt (master-slave) két számítógépes rendszer.

Az irányító számítógép (slave) végzi a közvetlen folyamatirányítási feladatokat: folyamatfelügye-letet, alapjelállító vagy közvetlen digitális szabályozást.

A felügyelő számítógép (master) az irányító számítógép számára optimális irányítási paramétereket számít ki, az irányítást befolyásoló parancsokat ad stb.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A párhuzamos működésű rendszerek rendszertechnikai felépítése az átkapcsolható tartalék rendszerekével megegyezik, lényeges eltérés van azonban az irányító és tartalék számítógép programrendszerében.

Minél jobban ki akarjuk használni a tartalék rendszer gépi lehetőségeit, annál nagyobb nehézségekkel kell számolni a programrendszer megvalósítása során.

Az átkapcsolás vezérlése a tartalékrendszerre lehet kézi vagy automatikus.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Az átkapcsolást hagyományos, illetve szilárdtest relékkel oldják meg.

A kézi átkapcsolást hibaészlelés és -jelzés után a kezelő kezdeményezi.

Automatikus átkapcsolás automatikus hibaészlelő áramkörökkel oldható meg.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A két számítógépes redundáns rendszerekben, párhuzamos működésű azonos funkciójú üzemben, a programmal történő összehasonlítás elvét alkalmazzák.

Egy hiba észlelése után, pl. ha a két számítógép számításainak eredménye nem egyezik, meg kell állapítani, hogy melyik gép a hibás.

Ezt két számítógép esetén mindkét módszernél rendszerint csak külön teszt-programok futtatásával lehet eldönteni.

MEGBIZHATÓSÁGI ALAPFOGALMAK

A gépi összehasonlítás kedvezően alkalmazható akkor, ha többségi, pl. a háromból kettő, összehasonlításra van lehetőség.

Ehhez három egyforma számítógéprendszer szükséges. Az összehasonlító egység ilyen esetben azokat az eredményeket fogadja el helyesnek, amelyek háromból legalább két számítógépnél megegyeznek.

A háromból kettő többségi elv így teszi lehetővé a hibás számítógép azonnali meghatározását.

MEGBIZHATÓSÁGI ALAPFOGALMAK

Egy többprocesszoros rendszer akkor redundáns kialakítású, ha az azonos típusú modulokból több van a rendszerben, mint amennyi a folyamatirányítási feladatok közvetlen ellátásához szükséges. Így a többletmodulok az alapmodulok tartalékai.

A vezérlő processzor meghibásodása ellen úgy lehet védekezni, hogy két processzorra bízzuk a vezérlést, s ezek egymást kölcsönösen ellenőrzik.

TÜV AJÁNLÁSOK

TÜV AJÁNLÁSOK

A mikroszámítógépes vezérlésekre a TÜV (Technische Überwachung Verein, Németországi Műszaki Felügyelőség) adott ki ajánlásokat a biztonság növelésére.

Ezek egy része a készülékek felépítésére, másik része a bevizsgálásra vonatkozik.

TÜV honlapja: www.tuv-fs.com/index.htm

TÜV AJÁNLÁSOK

TÜV tanúsítvány biztonsági elemekre / biztonsági alrendszerekre (ezek túlnyomó része elektromos, elektronikus, programozható elektronikus típusú) vonatkozó szabványai:

DIN V 19250/05.94 – Fundamental safety aspects to be considered for measurement and control equipment (Általános biztonsági szempontok, melyeket figyelembe kell venni mérő és vezérlő berendezések esetében);

TÜV AJÁNLÁSOK

DIN V VDE 0801/01.90 (with amendment A1: 1994-10 módosítással) – Principles for computers in safety-related systems (A biztonsági rendszerek számítógépeinek alapelvei);

IEC 61508, Part 1-7: Functional safety of E/E/PES safety-related system (Elektromos / Elektronikus / Programozható elektronikus biztonsági rendszerek funkcionális biztonsága)

TÜV AJÁNLÁSOK

A TÜV tanúsítvány tartalmazza azon szabványok listáját, amelynek egy elem / alrendszer megfelel.

A TÜV tanúsítvány megmutatja, hogy egy elem / alrendszer milyen sajátságos alkalmazásban felhasználható az ún. követelményi osztálynak (requirement class, RC) vagy a biztonsági integritási szintnek (safety integrity level, SIL) megfelelően.

TÜV AJÁNLÁSOK

EN 984-1 (safety categories):

„Safety of machinery -- Safety-related parts of control systems”

ISO 13849-1:2006 (performance level)

„Safety of machinery -- Safety-related parts of control systems -- Part 1: General principles for design”

TÜV AJÁNLÁSOK

IEC/EN 62061: 2005

„Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems” is the machinery specific implementation of IEC/EN 61508.

A RENDSZER ÁLTALÁNOS AJÁNLÁSAI

a) ***Mindig egy csatornával több legyen, mint amennyi a biztonságos működéshez legalább szükséges*:**

- **egy üzemelő csatorna és egy másik hasonló, amire hiba esetén át lehet kapcsolni (ez esetben átkapcsolás után már nincs redundáns csatorna),**
- **két csatorna + 1 tartalék azért, hogy a hiba esetén még mindig két csatorna szolgálja a biztonságot.**

A RENDSZER ÁLTALÁNOS AJÁNLÁSAI

b) A hibafelismeréssel kapcsolatos időkövetelményt ki kell elégíteni.

Az időkritérium nincs a biztonsági osztályokba beépítve, hanem csak az alkalmazástól függ.

Minden irányított folyamatnak van egy ún. hibatoleranciája.

Ez az az idő, aminek során a hibás jelet elviseli.

A RENDSZER ÁLTALÁNOS AJÁNLÁSAI

A vezérlés hibareakció-ideje (t_{hr}) kisebb kell legyen, mint az irányított folyamat hibatolerálási (t_{ht}) ideje, azaz $t_{hr} < t_{ht}$.

Olyan rendszereknél, ahol a biztonságos állapot nem rögtön érhető el, meg kell győződni arról, hogy a biztonsági állapot eléréséig nem kell-e újabb hibákkal számolni.

A RENDSZER ÁLTALÁNOS AJÁNLÁSAI

c) ***Mérlegelendő a megszakítások alkalmazása.***

Ezek közül azt kell kiválasztani, amely egyszerű rendszerfelépítést és tesztet tesz lehetővé.

Egymásba épített megszakításokat kerülni kell, csak az egyszintű megszakítás ajánlott.

A RENDSZER ÁLTALÁNOS AJÁNLÁSAI

***d) Speciális hardverek alkalmazását kerülni kell,* nehogy a rendszert lebénítsák.**

e) Hardverben rögzített címeket nem szabad használni és hibás alkalmazás ellen célszerű lebiztosítani.

Ha például az I8085-ös rendszerben nincs INT 7 megszakítás, vagy RST 7 utasítás, akkor az 38hex - 3Fhex: címek adatokkal tölthetők fel. Ha azonban valamilyen hardver- vagy szoftverhiba miatt mégis fellép az RST 7, akkor a program elszállhat. Ennek elkerülésére az 38hex címre olyan utasítást kell írni, amely direkt vagy indirekt hibajelzést ad.

A RENDSZER ÁLTALÁNOS AJÁNLÁSAI

f) ***Nem használt címeket alkalmazás ellen biztosítani kell.***

Az utasításszámláló (PC) vagy más címzést szolgáló regiszter hibájából olyan címzések fordulhatnak elő, amelyek nem használt memóriaterületeket érnek el.

Ezek elkerülésére a címek kiadásakor hibakezelő rutint kell indítani. Ezt ROM jellegű memóriák esetén programozással, RAM-nál inicializálással érik el.

A SZOFTVEREK ÁLTALÁNOS KÖVETELMÉNYEI

a) ***Nem engedhető meg nem teljes programlefutás.***

El kell kerülni, hogy egy hiba (pl. zavar a feszültségellátásban) csak valamilyen akciópár első felét hajtsa végre (pl. a szelep nyit-zár).

Újraindításkor először mindig a biztos állapot álljon elő, kifelé ható akciók csak a teszt lefutása után következhetnek.

A SZOFTVEREK ÁLTALÁNOS KÖVETELMÉNYEI

b) ***Általános programozási elvek.***

A TÜV számos ajánlást ad a programozásra.

Példa az az igény, hogy iterációs hurkoknál a leállási kritériumokhoz járulékosan egy maximális hurokfutási szám legyen előírva.

A SZOFTVEREK ÁLTALÁNOS KÖVETELMÉNYEI

c) ***Strukturált programozás.***

A biztonságtechnikában csak minőségileg nagy értékű szoftver alkalmazható, ami alatt a következődet értjük:

legyen alkalmazóbarát, hibamentes (az előírt kritériumoknak megfelelően), korrektsége könnyen vizsgálható, a tesztelése és a karbantartása egyszerű, változtatása könnyű valamint jól dokumentált.

A SZOFTVEREK ÁLTALÁNOS KÖVETELMÉNYEI

Egy program érvényessége és korrektsége megállapításánál fontos, hogy a program kisméretű, jól áttekinthető modulokból álljon, ezek a modulok egyszerűen legyenek konstruálva és a modulok között mindenkor egy összeköttetés legyen.

A SZOFTVEREK ÁLTALÁNOS KÖVETELMÉNYEI

Mindezek a strukturált programozással elérhetőek, miszerint a feladatot lépésen-kénti finomítással (top-down design) mindig csak a három struktúraelemmel, egyre kisebb részfeladatra kell bontani.

A SZOFTVEREK ÁLTALÁNOS KÖVETELMÉNYEI

A lebontás mindaddig folytatandó, amíg a részfeladatok jól áttekinthető egységre osztódnak, amit a programnyelven egyszerűen lehet programozni.

Az így kialakított program faszerkezete és egy-egy modul között csak egyetlen kapcsolat található.

A SZOFTVEREK ÁLTALÁNOS KÖVETELMÉNYEI

Különleges eseményekre (pl. vészkilépés) kivételek megengedhetők.

A lépésenkénti finomítással és az ebből származó faszerkezetnek az átláthatóság mellett az is előnye, hogy a megoldandó feladat a fejlesztés minden stádiumában és minden síkjában jól leírható.

A SZOFTVEREK ÁLTALÁNOS KÖVETELMÉNYEI

A lépésenkénti finomítás és a program faszerkezetének kialakításához a strukturált programozásban három struktúraelemet lehet alkalmazni:

- **sorrendek (következmények);**
- **hurkok;**
- **elágazások.**

A SZOFTVEREK ÁLTALÁNOS KÖVETELMÉNYEI

A sorrend (következmény) egy akciót ír le. Egy struktúraelem felbontható több egy-más után futó elem sorrendjére, amelyek önmagukban is egy struktúraelemet képezhetnek.

A huroknál egy vagy több struktúraelem annyiszor ismétlődik, ahányszor azt elő-írjuk.

Az elágazás két vagy több lehetséges folytatás közötti választási lehetőség.

A HARDVER ÁLTALÁNOS KÖVETELMÉNYEI

a) ***Az építőelemek csak specifikációjuknak megfelelően kerüljenek alkalmazásra.***

b) ***Kielégítő zavarvédettséget kell biztosítani.***

c) ***Feszültségfelügyelet*** **és** ***definiált viselkedés biztosítása*** **feszültségkimaradáskor és visszatéréskor.**

d) ***Két független időalap*** **alkalmazására azért van szükség, mert az időalap kiesése katasztrofális hibát okozhat.**

A TÁROLÓK ÁLTALÁNOS KÖVETELMÉNYEI

a) ***A programozható rendszereken a program integritása létfontosságú*****, ezért a programokat úgy kell tárolni, hogy változtatások ellen (feszültségkiesés, más külső hatás, hibás jelek) védve legyenek.**

A RAM tárolók tartalma, még ha teleppel feszültségkimaradás ellen védve is vannak, hibás beírójel vagy más külső hatásra (sugárzás, elektromágneses mezők) megváltozhat.

A TÁROLÓK ÁLTALÁNOS KÖVETELMÉNYEI

Programtárolóként csak fix tárolókat szabad alkalmazni, amelyekben az információ a lehetőségnek megfelelően elveszíthetetlen fizikai tulajdonság formájában van tárolva.

Ilyenek a ROM, EPROM, EEPROM.

Ha nincs fix tároló, intézkedni kell megfelelő tárolóvédelemről.

A TÁROLÓK ÁLTALÁNOS KÖVETELMÉNYEI

b) ***Dinamikus tárolót nem, vagy csak igen különleges esetben szabad alkalmazni.***

c) ***Háttértárolót nem szabad alkalmazni.***

AZ IRÁNYÍTÓ RENDSZEREK ALKALMAZÁSÁNAK BIZTONSÁGI OSZTÁLYAI

IRÁNYÍTÓ RENDSZEREK BIZTONSÁGI BESOROLÁSA

A DIN V 19250 szabvány tartalmazza az irányítórendszerek alkalmazásának biztonsági követelményeit.

Ez a szabvány az irányítórendszereket nyolc biztonsági (követelményi) osztályba sorolja.

IRÁNYÍTÓ RENDSZEREK BIZTONSÁGI BESOROLÁSA

Az 1. osztály jelenti a legalacsonyabb, míg a 8. a legmagasabb követelményeket.

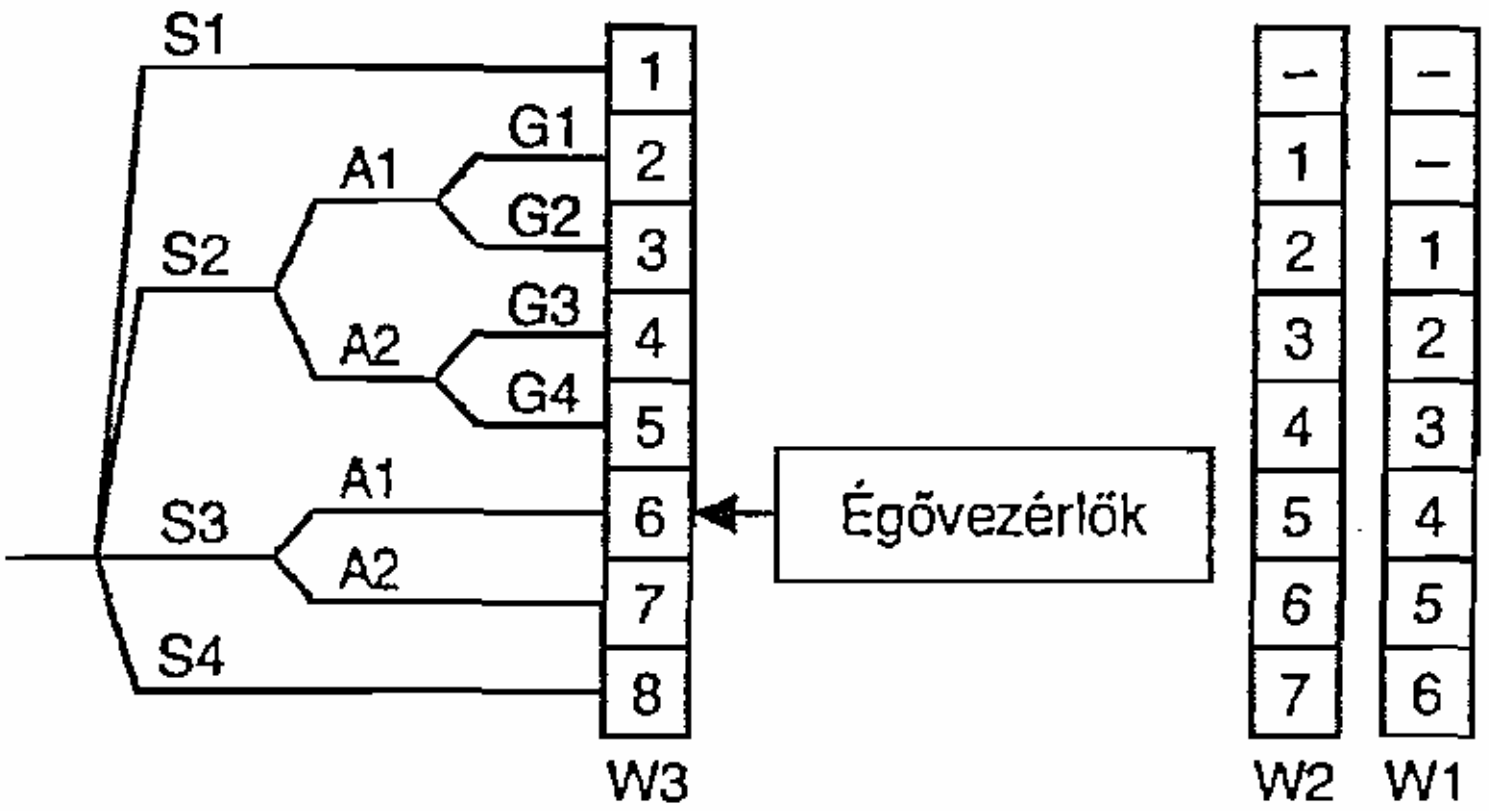
A szabvány *négy kockázatiparamétert* tartalmaz:

- ***veszélyesség nagysága* (extent of damage), S**
  - **S1 kisebb sérülés;**
  - **S2 több személy súlyosabb sérülése, vagy egy személy halála;**
  - **S3 több személy halála;**
  - **S4 katasztrófa jellegű esemény.**

IRÁNYÍTÓ RENDSZEREK BIZTONSÁGI BESOROLÁSA

- ***veszélyes területen tartózkodás előfordulása (duration of stay in hazardous area), A***
  - **A1 soha, nagyon ritkán, vagy időnként;**
  - **A2 gyakran, vagy állandóan.**
- ***veszélymegelőzés* (danger prevention), G**
  - **G1 lehetséges;**
  - **G2 nem lehetséges.**
- ***az előfordulás valószínűsége* (probability of occurrence), W**
  - **W1 igen alacsony;**
  - **W2 alacsony;**
  - **W3 relatív magas.**

IRÁNYÍTÓ RENDSZEREK BIZTONSÁGI BESOROLÁSA



Irányító rendszerek biztonsági besorolása

IRÁNYÍTÓ RENDSZEREK BIZTONSÁGI BESOROLÁSA

Például hatos veszélyességi követelmények az égővezérlések, az utasszállító rendszerek (metró, vasút), a közúti forgalomirányító rendszerek és a gázfeldolgozó rendszerek területein találhatók.

Az elektromos, elektronikus, ill. programozható elektronikus rendszerek (E/E/PES) követelményeit az 1997-ben elfogadott IEC 61508 nemzetközi szabvány foglalja össze a legátfogóbban a növelt biztonságot igénylőipari alkalmazásokhoz.

BIZTONSÁGI PLC-K RENDSZERTECHNIKÁJA

BIZTONSÁGI PLC-K RENDSZERTECHNIKÁJA

A veszélyes technológiák vezérlésére használható PLC-ket a zsargonban biztonsági PLC-knek nevezik.

Az ipari biztonsági PLC-k a normál PLC-k redundanciáján, ill. a speciális, növelt biztonsági PLC-k redundanciáján alapuló felépítést követi.

BIZTONSÁGI PLC-K RENDSZERTECHNIKÁJA

A biztonsági PLC-k a technológia veszélyességéhez igazodóan alapvetően kétféle algoritmus szerint viselkednek a hiba felismerésekor:

- **hibatűrő PLC (fault-tolerant), azaz működésbiztos;**
- **veszélybiztos PLC (fail-safety).**

Mindkét esetben a biztonság növelését a redundancia növelésével érik el.

HIBATŰRŐ PLC RENDSZER

A hibatűrő PLC rendszer esetén két darab PLC mindig szinkronizáltan és párhuzamosan, egymással kommunikációs kapcsolatban működik.

Közülük az egyik az aktív, amelyik irányítja a folyamatot, a másik PLC passzív, de a kommunikációs kapcsolat révén bármikor átveheti a folyamat irányítását (hot-standby).

HIBATŰRŐ PLC RENDSZER

A hibatűrő PLC rendszer alkalmazásának elsődleges célja a technológiai folyamat végrehajtása.

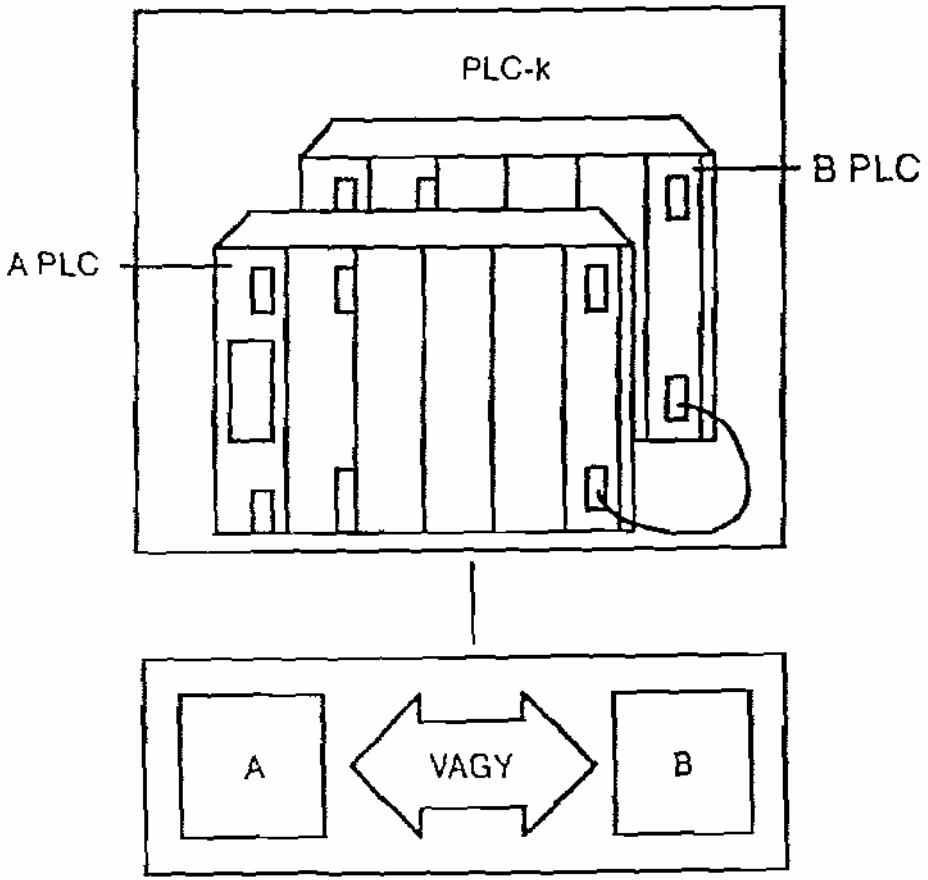
Amennyiben az aktív PLC meghibásodása esetén a passzív PLC átveszi a folyamat irányítását (aktívvá válik), akkor a rendszer már nem hibatűrőként viselkedik, mivel nincs tartalék PLC a rendszerben.

HIBATŰRŐ PLC RENDSZER

A hibatűrő PLC alkalmazható a gyógyszeriparban, az élelmiszeriparban, acélművekben vagy olajipari technológiák irányításban.

Általában ott célszerű alkalmazni, ahol a vezérlőberendezés meghibásodása esetén a technológiai folyamat leállítása igen költséges és ugyanakkor a technológia alacsony veszélyességi fokozatú.

HIBATŰRŐ PLC RENDSZER



A hibatűrő PLC VAGY analógiája

HIBATŰRŐ PLC RENDSZER

Az előző dia a nem veszélybiztos működésű, hibatűrő PLC működését szemlélteti.

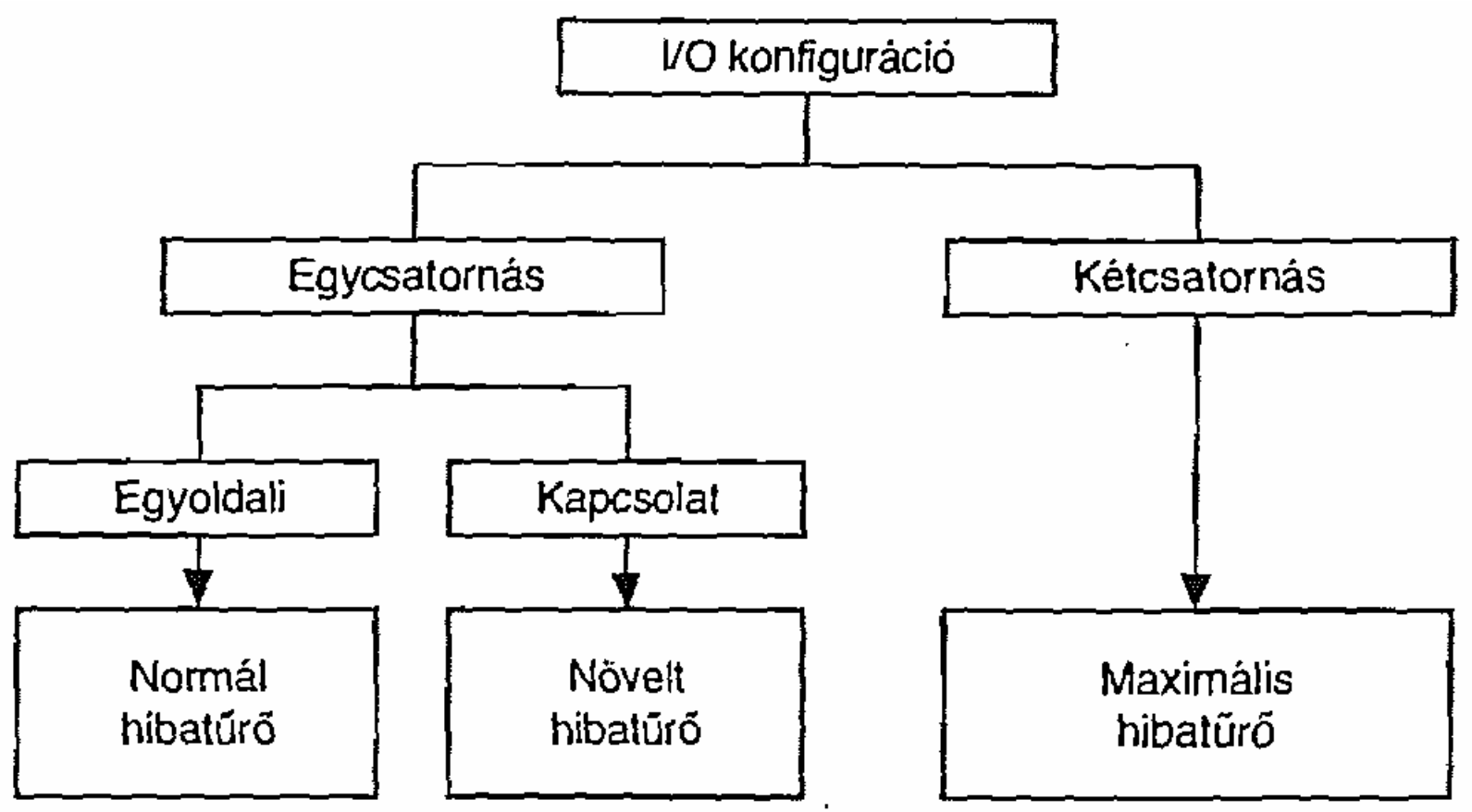
E szerint a két PLC (A és B) működése a VAGY művelethez hasonlítható, miszerint ha legalább az egyik PLC üzemképes, akkor a vezérlőrendszer működőképes.

HIBATŰRŐ I/O KONFIGURÁCIÓ

A PLC-k biztonságának növelése az I/O eszközökre is fokozott biztonságot követel.

A hibatűrésnek három különböző szintje lehetséges az I/O modulok konfigurációjától függően.

HIBATŰRŐ PLC RENDSZER



A hibatűrő I/O konfigurációk

HIBATŰRŐ I/O KONFIGURÁCIÓ

- ***normál hibatűrés*** **(normal fault tolerance, single side configuration);**
- ***növelt hibatűrés*** **(enhanced fault tolerence, switched configuration);**
- ***maximális hibatűrés*** **(maximum fault tolerance, fully redundant configuration).**

HIBATŰRŐ PLC-KONFIGURÁCIÓ KOMMUNIKÁCIÓS FUNKCIÓI

a) *Adatcsere és hibakezelés*

A hibatűrő konfigurációjú PLC-k melegtartalék (hot standby) üzemmódban működnek.

Ha hiba keletkezik, akkor a másik alegység, a tartalék veszi át a folyamat irányítását. A hibás alegységet ki lehet javítani a folyamat megszakítása nélkül. Kétcsatornás I/O konfigurációban mindkét alegység párhuzamosan működik.

HIBATŰRŐ PLC-KONFIGURÁCIÓ KOMMUNIKÁCIÓS FUNKCIÓI

Melegtartalék esetében az a cél, hogy a tartalék időkiesés nélkül vegye át a folyamat irányítását.

Ehhez az szükséges, hogy mindkét egység alkalmas legyen igen gyors és megbízható adatcserére.

Mindkét alegységnek tartalmaznia kell ugyanazt a felhasználói programot, adatblokkot és I/O állapotinformációt.

HIBATŰRŐ PLC-KONFIGURÁCIÓ KOMMUNIKÁCIÓS FUNKCIÓI

b) *Szinkronizáció*

Az aktív és passzív egység közötti adatcseréhez a két alegység szinkronizációja szükséges, ez az eseményvezérelt szinkronizáció.

Eseményvezérelt szinkronizáció megy végbe, amikor egy esemény okoz valamilyen váltást az alegységek állapotában, pl. parancsok az I/O-kra, blokkhívó parancsok vagy időfunkciójú parancsok.

HIBATŰRŐ PLC-KONFIGURÁCIÓ KOMMUNIKÁCIÓS FUNKCIÓI

c) Önteszt

A következő funkciókat és komponenseket tesztelik: belső buszrendszer, központi vezérlővonal, hibalokalizáló rendszer, CPU-k és memóriák.

Valamennyi hibadetektálást az önteszt idején jelez a rendszer.

Újraindításkor valamennyi alegységen végigfut az öntesztes ellenőrzés.

HIBATŰRŐ PLC-KONFIGURÁCIÓ KOMMUNIKÁCIÓS FUNKCIÓI

Ciklikus üzemmódban az operációs rendszer indítja az önteszt funkcióját közelítőleg 5 ms-nyi intervallumokban, amelyek száma a felhasználó által programozható.

VESZÉLYBIZTOS PLC-KONFIGURÁCIÓ

Ahol a biztonságos működés az első számú követelmény a technológia veszélyessége miatt, mint például a kazánautomatikák, vasúti szerelvények automatizálása, gáz-és olajszállítással kapcsolatos automatikák, vegyipar, nukleáris erőművek stb., ott a veszélybiztos PLC-konfiguráció szükséges.

VESZÉLYBIZTOS PLC-KONFIGURÁCIÓ

A veszélybiztos rendszer alapkonfigurációban igen hasonlít a hibatűrő rendszerekhez, mivel két alapegység működik egymással összekapcsolva.

A fő különbség az, hogy a veszélybiztos változatban a két alapegység folyamatosan összehasonlítja egymás állapotait, eredményeit és megelőzi a veszélyes válaszok kijutását.

VESZÉLYBIZTOS PLC-KONFIGURÁCIÓ

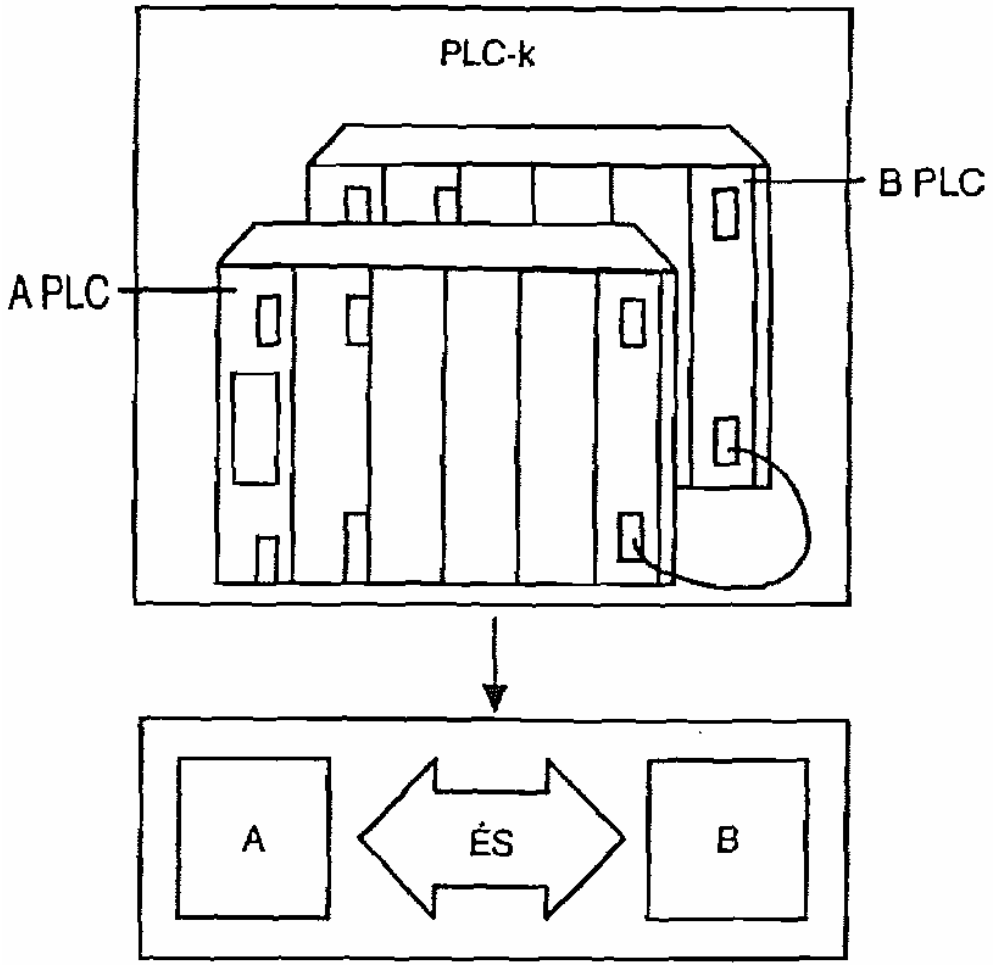
A veszélybiztos PLC-k kielégítik a DIN V 19250 szabvány hatos osztályú követelményeit.

A veszélybiztos PLC nem hibatűrő.

A veszélybiztos PLC alkalmazásának célja *megelőzni a hibás működési feltételeket* és nem az, hogy elkerülje a technológiai folyamat leállítását.

A veszélybiztos működési elv a redundáns alegységek ÉS kapcsolatán alapul.

VESZÉLYBIZTOS PLC-KONFIGURÁCIÓ



A hibatűrő PLC ÉS analógiája

VESZÉLYBIZTOS PLC-KONFIGURÁCIÓ

A veszélybiztos működést a PLC a következő funkciókkal éri el:

- **öntesztelés az operációs rendszerrel;**
- **az I/O-k speciális külső veszélybiztos kialakítása;**
- **kétcsatornás redundáns struktúra az eredmények állandó összehasonlítására.**

VESZÉLYBIZTOS PLC-KONFIGURÁCIÓ

A veszélybiztos redundáns PLC rendszer két központi egységének funkciói:

- **adatcsere és válasz a hibára;**
- **szinkronizáció;**
- **önteszt.**

BIZTONSÁGI PLC-K I/O KONFIGURÁCIÓI

BIZTONSÁGI PLC-K I/O KONFIGURÁCIÓI

A hibatűrő, ül. veszélybiztos PLC-k esetén a CPU működése mellett a be/kimeneteknek is fokozott követelményeknek kell megfelelni.

A biztonsági bemeneteknél a biztonsági program futása alatt meg kell győződni arról, hogy a „0" logikai szintre a bemenetek működőképesek-e.

(Szakadásra végre tudja-e hajtani a lekapcsolást).

BIZTONSÁGI PLC-K I/O KONFIGURÁCIÓI

A biztonsági kimeneteknél a biztonsági program futása alatt kell megvizsgálni (visszacsatolással vagy egyéb úton), hogy a „0" logikai átmenetre a végrehajtó szervek áramkörei (és esetleg a saját bemenetei) működőképesek-e.