Értékünk az ember

Humánerőforrás-fejlesztési Operatív Program

Farkas György – Héray Tibor

MINŐSÉG ÉS MEGBÍZHATÓSÁG

SZÉCHENYI ISTVÁN EGYETEM
GYŐR

Magyarország célba ér
NEMZETI FEJLESZTÉSI TERV

Készült a HEFOP 3.3.1-P.-2004-09-0102/1.0 pályázat támogatásával.

Szerzők: dr. Farkas György
főiskolai tanár

dr. Héray Tibor
főiskolai docens

Lektor: dr. Tarnai Géza
egyetemi tanár

A dokumentum használata

Mozgás a dokumentumban

A dokumentumban való mozgáshoz a Windows és az Adobe Reader megszokott elemeit és módszereit használhatjuk.

Minden lap tetején és alján egy navigációs sor található, itt a megfelelő hivatkozásra kattintva ugorhatunk a használati útmutatóra, a tartalomjegyzékre, valamint a tárgymutatóra. A ◀ és a ▶ nyilakkal az előző és a következő oldalra léphetünk át, míg a Vissza mező az utoljára megnézett oldalra visz vissza bennünket.

Pozícionálás a könyvjelzőablak segítségével

A bal oldali könyvjelző ablakban tartalomjegyzékfa található, amelynek bejegyzéseire kattintva az adott fejezet/alfejezet első oldalára jutunk. Az aktuális pozíciónkat a tartalomjegyzékfában kiemelt bejegyzés mutatja.

A tartalomjegyzék használata

Ugrás megadott helyre a tartalomjegyzék segítségével

Kattintsunk a tartalomjegyzék megfelelő pontjára, ezzel az adott fejezet első oldalára jutunk.

Keresés a szövegben

A dokumentumban való kereséshez használjuk megszokott módon a Szerkesztés menü Keresés parancsát. Az Adobe Reader az adott pozíciótól kezdve keres a szövegben.

Tartalomjegyzék

Előszó

A könyv elsősorban a BSc szakok számára készült tankönyv tankönyv, de az volt a cél, hogy a gyakorló mérnök és a menedzser részére bevezető szintű szakkönyvként is alkalmazható legyen. Ezért egyes anyagrészek olyan alapvető elméleti ismereteket és gyakorlati tudnivalókat tartalmaznak, amelyek valamennyi, a témával még csak felületesen ismerkedőnek is nélkülözhetetlen. Más fejezetek, részletek a témában jobban elmélyedőknek készültek.

A szöveges részeken túl a matematikai formában megadott összefüggések értelmezése, alkalmazni tudása a mérnök szintjén követelmény, ezért a téma tárgyalásakor matematikai, valószínűség számítási ismereteket fel kellett tételeznünk. Az olvasók egy része esetleg nélkülözni tudja a képletek bizonyítását, levezetését. Ezeket kissé elkülönítve közöljük, hogy aki nem kíván ebben elmélyedni, (illetve bizonyítás nélkül is „hisz"), az az első olvasáskor a kissé bonyolultabb levezetéseket átugorhassa.

A könyv három jól elhatárolható témakört ölel fel: foglalkozik a megbízhatóság- és biztonság-elmélet alapjaival és összefoglalja a minőségbiztosításra vonatkozó alapvető ismereteket is. A megbízhatóság és biztonság fogalmát a mindennapi életben is gyakran használjuk. A megbízhatóság esetén valamely rendszer meghibásodásának, a biztonság esetén pedig a veszélynek, vagy végső soron a kár bekövetkeztének az elkerülése a cél. A megbízhatóság és biztonság egymástól eléggé függetlenül is jelentkezhet. Valamely műszaki eszköz lehet biztonságos és mégis kevéssé megbízható (például egy olyan autó, amely nehezen indítható), hasonlóan előfordulhat, hogy adott eszköz nagy megbízhatóságú, de nem biztonságos (például egy autó nagyon ritkán hibásodik meg, de meghatározott meghibásodás esetén, például egyszerűen kivitelezett fékrendszer esetén közvetlen veszélyhelyzet lép fel). Ilyen esetben tehát állandóan aggódhat az autó tulajdonosa, hogy nehogy ez a meghibásodás lépjen fel. Csak abban az irreális esetben lenne egy rendszer egyidejűleg megbízható és biztonságos, ha egyáltalán nem kellene meghibásodással számolni.

A megfelelő megbízhatóság és biztonság elérésére különböző intézkedések képzelhetők el, melyek alapja az előbbi esetben a rendszer gazdaságos kialakítása, utóbbiban pedig annak az engedélyező hatóság által történő elfogadása. A megbízhatóság növelésére hozott intézkedések a hibák fellépésének esélyét kívánják csökkenteni, a biztonságnövelés célja a hibák

veszélyes hatásának kiküszöbölése lehet, hisz teljesen hibamentes rendszer nem képzelhető el. A megfelelően nagy megbízhatóság igazolása a megbízhatóság-elmélet számítási módszerei segítségével végezhető el, gyakran azonban egy megfelelően nagy garanciaidő megadásával adnak jellemzést a megbízhatóság szintjéről.

A biztonság növelésére hozott intézkedések esetén más a helyzet, a biztonsági szint igazolására általában az engedélyező hatóság részéről szükséges üzembevételi engedélyt beszerezni. Ehhez egy megfelelő biztonságigazolási eljárást kell végrehajtani.

Itt jegyezzük meg, hogy a könyv teljes terjedelme nem teszi lehetővé, hogy olyan elméleti és gyakorlati részletekre is kiterjedjen, amely minőségbiztosítási, megbízhatósági, biztonság-technikai területen szakértői szinten szükséges. Az olvasó figyelmébe ajánljuk a mellékelt irodalom jegyzéket.

Gyakran megadjuk az egyes szakkifejezések angol, német és orosz megfelelőjét (a magyar után ebben a sorrendben). Ez nemcsak azoknak hasznos, akik ezeken a nyelveken írt szakirodalmat olvassák, hanem mivel beszerzéskor a termék specifikációja rendszerint nem áll rendelkezésre magyarul, az adatok értelmezhetőségéhez a kifejezések ismerete nem nélkülözhető.

Az egyes fejezetekben szereplő példák és feladatok segítségével az olvasó maga ellenőrizheti az anyag megértését, ugyanakkor ezek fontos kiegészítéseket is tartalmaznak, ezért semmiképpen nem nélkülözhető részt képeznek.

Néhány függvény jelölése

Σ (...)	összeg (szumma)
Π (...)	szorzat (produktum)
A ... Z	vektorok, elemei szögletes zárójelben [ ]
$\hat{X}$	az X empirikus, becsült értéke

Az operátor után kapcsos zárójelet használtunk: { }

M{...}	átlagérték
Pr{...}	valószínűség

1. A minőséggel kapcsolatos általános követelmények

A megbízhatóság-elmélet az a tudományág, amely a működtetés ideje alatti maximális hatékonyság biztosítására a termékek tervezése, gyártása, átvétele, szállítása és felhasználása során betartandó általános módszereket és eljárásokat tanulmányozza, valamint kidolgozza a berendezések minőségének ismert mutatók alapján történő számítás módszereit. Megállapítja a berendezésekben fellépő meghibásodások keletkezésének törvényszerűségeit, előrejelzésének módszereit, keresi a termékek megbízhatóságának növelési lehetőségeit a tervezés és gyártás során, a megbízhatóság fenntartását segítő módszereket a tárolás és felhasználás ideje alatt, kidolgozza a termékek megbízhatóságának ellenőrzési módszereit, a megbízhatóság ellenőrzésére alkalmazandó eljárásokat, a termelés, gyártás minőségének számszerű mutatóit. Fentiek alapján látható, hogy a megbízhatóság-elmélet a mérnökök, fizikusok, vegyészek, közgazdászok hatáskörébe tartozó igen komplex tudományág. Számos kérdése ismert matematikai módszerek alkalmazását igényli – fontos a valószínűség számítás és a matematikai statisztika módszereinek ismerete.

A megbízhatóság-elmélet gyakran egymásnak ellentmondó feladatokkal kerül szembe. A berendezések funkcióinak bővülésével azok egyre bonyolultabbak lesznek, egyre több alkatrészből építhetők fel – ami a megbízhatóság csökkenéséhez vezet. A feladatok fontosságának növekedése miatt azonban egyre nagyobb megbízhatóságot követelünk ezektől a berendezésektől. Az ellentmondás feloldására szükséges a megbízhatóság növelése megfelelő alkatrészek, megfelelő struktúrák, konstrukciós megoldások stb. alkalmazásával.

A komplex rendszereknél a megfelelő minőség eléréséhez általában nem elegendő, ha a készülék vagy rendszer az átadás pillanatában hibátlan. A rendszerek meghibásodásából adódó problémák, a növekvő fenntartási költségek növekedése, a speciális képzettségű kezelő és karbantartó személyzetben jelentkező hiányok miatt a megbízhatóság, karbantarthatóság, üzemkészség és biztonság kérdése egyre jelentősebb.

A minőség- és megbízhatóság-biztosítás korszerű módszerei segítségével vizsgálhatók a fentiekhez hasonló kérdések. A teljesítményparaméterek, a működésjellemzők és a költségek közötti optimum megtalálása fontos célkitűzése a megbízhatósági vizsgálatoknak.

A műszaki termékek biztonsági és megbízhatósági követelményeinek teljesítése olyan szakmai feladat, amelynek szerves, szoros gazdasági vonatkozásai vannak. A minőségről az árak nélkül csak igen kivételes esetekben lehet döntéseket hozni. A minőség, a megbízhatóság és a biztonság tehát egyszerre műszaki és gazdasági kérdés. Egy gyártmány előállítója, forgalomba hozója, beruházója, üzemeltetője nem nélkülözheti a termék minőségi, megbízhatósági, biztonsági jellemzőit, ezért fontos, hogy az alapvető fogalmakkal tisztában legyen, tudja értelmezni a specifikációt beszerzés esetén és ebből a szempontból is össze tudja hasonlítani a számításba jövő gyártmányokat. A termék tervezőjével, konstruktőrével szemben pedig alapvető elvárás, hogy adott minőségi és gazdasági követelményeket kielégítő terméket hozzon létre.

A műszaki élet speciális területét jelentik a biztonságkritikus rendszerek, amelyeknél a megbízhatóságon kívül a biztonság is fontos minőségi jellemző. A biztonság tágabb értelemben veszélymentességet jelent, pontosabb meghatározásával később (a 8. fejezetben) foglalkozunk. A biztonság fogalma rendkívül fontos a műszaki életben, amit mutat az is, hogy az ember pszichológiai igényei között a legfontosabbak közt szerepel. E pszichológiai igények Maslow-féle hierarchiájában a fiziológiai igények után rögtön a biztonság iránti igény szerepel (1-1. ábra). Ezt a műszaki rendszerek vizsgálata során mindenképpen szem előtt kell tartani.

1-1. ábra: Az ember pszichológiai igényeinek Maslow-féle hierarchiája

A megbízhatóság- és biztonságelmélet egyaránt a hibákkal, meghibásodásokkal kapcsolatos kérdéseket vizsgálja. A megbízhatóságnak és a biztonságnak egyaránt ismeretes a köznapi és műszaki értelmezése. Műszaki értelmezésben mindkettő valószínűségi jellegű számszerű jellemzőt jelent, ami az adott időpontbeli hibátlan állapot valószínűségét adja meg. A megbízhatósági vizsgálatoknál valamennyi – a vizsgált egységgel kapcsolatban

előforduló – hibát számításba kell venni. E hibákat következményük alapján két csoportra oszthatjuk és beszélhetünk csupán üzemzavart eredményező ún. akadályozó-, illetve veszélyes hibákról. A biztonsági vizsgálatoknál csupán ez utóbbi, veszélyes hibákat vesszük figyelembe.

A követelményeknek megfelelő minőséget, megbízhatóságot, üzembiztonságot a tervezés időszakaszában a megfelelő struktúrával, konstrukcióval és technológiával kell biztosítani. A gyártáskor nem lehetséges, vagy legalább is túl költséges egy konstrukció-módosítás, a felhasználás során pedig már meghibásodások, üzemkiesések keletkezhetnek a nem kielégítő megbízhatóság miatt. Az utólagos módosítások, kiegészítések mindig sokkal költségesebbek, esetleg már nem is orvosolható a tervezési hiányosság, ha azt az üzemeltetés, alkalmazás során kell megoldani, nem is beszélve a biztonság nem kielégítő mértéke miatt esetleg bekövetkező katasztrófáról.

Nemcsak a biztonságkritikus berendezések esetében (mint például atomerőművek, űrhajók, vasúti biztosító berendezések, számítógépes irányító rendszerek stb.) szükséges a termékek megbízhatósági, biztonsági analízisét elvégezni, bár ezeknél kétségtelenül elsődleges fontosságú. A kommersz háztartási elektromos és elektronikus készülékeket is szükséges megbízhatósági szempontoknak megfelelően tervezni, illetve a terméket ebből a szempontból vizsgálni, mert e nélkül nem lehet felelősséggel garanciát vállalni egy termékre, nem lehet a szervizét megtervezni, a szükséges tartalékkészleteket kiszámítani.

Míg a biztonságkritikus rendszereknél az élet- és vagyonbiztonság teszi szükségessé a megbízhatóság menedzselését, a kommersz termékek esetében „csak" gazdasági természetű követelmények kényszerítik rá a tervezőt, gyártót, felhasználót arra, hogy a kérdéssel behatóan foglalkozzék. Ma már közel valamennyi gyártmány értékesíthetőségének elengedhetetlen feltétele, hogy a minőség biztosítása nemzetközileg elfogadott és ellenőrzött szabályoknak feleljen meg, hogy a megbízhatóságot megfelelően specifikálják és természetesen az előírt megbízhatóság-szintet szavatolják is. Ezzel kapcsolatban a minőség és komponenseinek vizsgálata alapvetően kétféle szemléletben végezhető. A **mérnöki szemlélet** szerint alapvető feladatnak azt tekinthetjük, hogy adott termék, rendszer stb. minőségét, megbízhatósági illetve biztonsági szintjét meg tudjuk határozni és lehetőleg mennyiségi, számszerű jellemzőt tudjunk hozzárendelni. Ugyanezen kérdéskör **menedzser-szemléletű** vizsgálata azt jelenti, hogy ismertnek feltételezve a kívánt minőségi (megbízhatósági, biztonsági) szintet, hogy lehet azt az életciklus különböző fázisaiban elérni.

A műszaki élet egyre több területén használják az eredetileg főleg biológiában használatos **életciklus** fogalmat, értve alatta a rendszer teljes élettartama alatt előforduló életszakaszokat (a rendszerkoncepció kialakításától a rendszerterv kialakításán, konstrukciós és egyéb tervezésen, kivitelezésen, tesztelésen keresztül az üzemeltetésig, sőt a rendszer üzemidejének lejárta után annak megsemmisítéséig). A következőkben mi is gyakran fogjuk ezt a fogalmat használni.

Igen komoly anyagi érdekellentétek sőt, jogi viták jelentkeznek egy az átvevő által nem megfelelőnek talált szállítmány visszautasíthatóságával kapcsolatosan. Esetenként igényes matematikai számításokat kell elvégezni ahhoz, hogy lássuk, mekkora az átvevő kockázata, ha jónak minősít egy nem megfelelő szállítmányt és viszont, mekkora az átadó kockázata, ha visszautasítják a megfelelő terméket. A szállítmány mekkora hányadának hibáját kell még elfogadni, mikor utasítható vissza a teljes egész? Ki vizsgálja a terméket az átadó, vagy az átvevő, vagy mindkettő? Ilyen és számos hasonló kérdésre kell a gyakorlatban jogi szabályozás, szerződéses kikötés, amelyek csak valószínűség számítási módszereken, matematikai statisztikai számításokon alapulhatnak.

2. Megbízhatósági alapfogalmak

2.1. Fogalom meghatározások

A következőkben alkalmazott alapfogalmak a nemzetközi szakirodalomnak, illetve a vonatkozó szabványoknak általában megfelelnek. Eltérés akkor adódhat, ha az utóbbiak nem egységesek és/vagy bonyolultságuk e könyv tárgyalás módját meghaladja. A fogalom fejlődése kb. a 70-es évek közepén került abba az állapotba, hogy a szabvány az eredeti hibamentességként értelmezett fogalma helyett már más tényezőket is figyelembe vegyen, így az MSZ 292–76 sz. szabvány a megbízhatóság alábbi összetevőit definiálja:

- **hibamentesség,**
- **tartósság,**
- **javíthatóság,**
- **tárolhatóság.**

Jó egy évtizeddel később az MSZ IEC 50(191):1992 sz. szabvány a megbízhatóságot a következőképpen határozta meg:

Gyűjtőfogalom, amelyet a használhatóság és az azt befolyásoló tényezők, azaz a hibamentesség, a karbantarthatóság és a karbantartás-ellátás leírására használnak.

A továbbiakban általában a szabványokban is szokásos egyszerűsítéssel döntően a **hibamentesség**gel foglalkozunk, az erre vonatkozó jellemzőket és összefüggéseket vizsgáljuk. A tárolhatósággal, tartóssággal kapcsolatos elemzésekre lehetőséget adnak a stresszre vonatkozó részek, valamint a meghibásodási tényező időfüggését tárgyaló fejezet. A javíthatóságra a determinisztikus jellemzőknél térünk ki.

A minőség, megbízhatóság, biztonság szempontjából vizsgált **objektum** általában valamilyen **termék.** A mezőgazdasági, vegyipari termékek is ide tartoznak, de ebben a könyvben csak **műszaki termék**ekkel foglalkozunk, ezen belül is döntően **elektronikus** alkatrészekkel, készülékekkel, biztonságkritikus rendszerekkel és érintőlegesen a szoftverrel. A tárgyalás kiterjed az egyszerű alkatrésztől, a nagyobb funkcionális egységekig. Az ismertetett módszerek vonatkoznak készülékre, berendezésre, bonyolult rendszerre, sőt az ilyen rendszerekkel nyújtott szolgáltatásra is. Az általánosság kedvéért a vizsgálat tárgyát, a hardver- vagy szoftver-terméket, illet-

ve az analizált rendszert, szolgáltatást **objektum**nak nevezzük. (Más irodalmakban a szerződési modellre alapozva szokás **átadandó**ról beszélni.)

Egy objektum **minősége** az értéket képviselő tulajdonságairól alkotott értékítélet. Lehet az **érték** használati, piaci, esztétikai; az **ítélet** szubjektív, objektív. A kereskedő értékítélete például általában szubjektív és a vásárló értékelését tükrözi. A **műszaki minőség** használati és objektív értékelésen, döntően mérhető (összehasonlítható, adott skála szerint rendezhető, számszerűsíthető) mennyiségeken alapul.

Az objektum műszaki tulajdonságai mérhető, vagy számítható adatokkal, objektív **paraméterekkel** jellemezhetők. A paraméterekre vonatkozó előírás a **specifikáció,** ez és az alkalmazás feltételei (a használati utasítás) szervesen kapcsolódnak egymáshoz.

Az objektum műszaki **minőségét** a paraméterek és a specifikáció viszonya határozza meg. A legegyszerűbb esetben **„jó"**-nak tekintjük a terméket, ha a paraméterei a specifikáció által meghatározott **tűréstartományon** belül vannak. A jó és a rossz állapotot elhatároló **hibakritérium**-ot azonban egy adott alkalmazásban, adott funkciók teljesülése alapján és nem feltétlenül a gyártmány teljes specifikációja szerint kell értelmeznünk. Gondoljunk arra, hogy egy a tökéletestől eltérő állapotú termék még kielégítheti az igényeket és ekkor sem hibátlannak, sem rossznak nem célszerű tekinteni. (Például, ha olyasmi vált benne működésképtelenné, amire az adott alkalmazásban soha sincs szükség.) Ilyenkor nem egyértelmű a hibakritérium, vagy nemcsak egyféle kritériumot kell értelmezni. Végső soron, amikor a számításainkban csak kétféle állapotot különböztetünk meg, mindig az adott alkalmazás a mérvadó a hibakritériumra.

Az esztétikai követelmények nem teljesülésekor is használható lehet a termék. Meg kell továbbá jegyeznünk, hogy a paraméternek a tűrési tartományból a kedvezőbb irányba való kilépését – tehát, ha az nem korlátozza, sőt bővíti a felhasználást – gyakran nem tekintjük jó állapotnak. Például egy műszer mérési pontossága a specifikált mérési tartományra vonatkozik. A mérési tartomány határain kívül is működő eszköz pontossága ott esetleg igen rossz és ez a felhasználót megtévesztheti. Avagy ha egy tápegységnek a specifikált maximális terhelés túllépésekor ki kell kapcsolnia, de ezt nem teszi, hanem nagyobb árammal is működik, az sok problémát okozhat, annak ellenére, hogy többet tud, mint amire eredetileg való.

Bonyolult, többfunkciójú berendezések, komplex rendszerek és szolgáltatások esetében rendszerint egyáltalán nem célszerű csak **„jó-rossz”** állapotokról beszélni. A paraméterek lehetséges értéktartományát e kettőnél **több diszjunkt résztartományra** kell osztani, mivel az előző kategorizálás a minőségnek egy túlzottan durva leírására adna csak módot, ami a kiértékelésnél nem elegendő. A jó és rossz jelzők helyett készülékek, szolgáltatások esetén az adott alkalmazásra értelmezett **„üzemképes – üzemképtelen”** vagy a szakzsargonban szokásos „**up – down”** elnevezést használjuk.

Az irodalomban a hibára, meghibásodásra nem egységes a szóhasználat. Alkatelemekre és összetett egységekre is eltérő. Példa: **„fault tolerant”** struktúra esetén nem minden **„defect”** okoz **„errort”.** Egy lehetséges – de korántsem egységes – szóhasználat: a meghibásodás **(failure)** miatt bekövetkező hiba **(fault)** okozhat eltérést a specifikációtól **(error),** ami a funkcionális követelmények nem teljesülésüléséhez **(defect)** vezet. A továbbiakban a hibás állapotot általában a fault értelmében használjuk, a működésképtelenséget a defect értelmében.

A vizsgált objektum **jó-állapotát** hibák, meghibásodások, illetve zavarok miatt hagyhatja el. A hibák és meghibásodások sok szempont szerint osztályozhatók, minden esetre célszerű lehet egy olyan csoportosítás, amely az okok szerint történik. Ilyen módon két alapvető kategóriát különböztethetünk meg:

a) **Fizikai hatások következtében fellépő meghibásodások** fajtái:

- alkatrész meghibásodások,
- konstrukciós hiba,
- gyártástechnikai hiányosság,
- az előírásost meghaladó környezeti terhelés,
- az előírásost meghaladó funkcionális igénybevétel (túlterhelés),
- az előírásos használat során bekövetkező öregedés (elhasználódás),
- szoftver hibák véletlen hardver meghibásodások miatt,
- természetes eredetű elektromágneses zavarok.

E meghibásodások befolyásoló tényezői:

- gyártási mód (például a gyártási tűrések nagysága),
- környezeti feltételek (például agresszív atmoszféra),
- terhelés nagysága, amely öregedéshez, elhasználódáshoz vezethet.

A hibamechanizmusok fenti befolyásoló tényezőivel részletesen a megbízhatóság technika „megbízhatóság-fiziká”-nak nevezett részterülete foglalkozik.

b) **Emberi tevékenységre visszavezethető hibák fajtái:**

- a feltétfüzet specifikációs hibái (melyről a későbbiekben részletesebben is szó lesz)
- tervezés során elkövetett hibák
  - szoftverhiba a rendszertervben
  - hiba a programírásban,
  - hardver-tervezési hiba
  - más objektumokból származó elektromágneses zavarok,
  - hiba a dokumentációban,
- hardver megvalósítási hiba (kivitelezés során)
- kezelési és adatbeviteli hiba,
- fenntartási hiba,
- tárolási hiba,
- szándékos hibák (vandalizmus, szabotázs, lopás).

Műszaki szempontból **hiba** vagy **meghibásodás** jelentkezik, ha a vizsgált egység meghatározott számjellemzőjének tényleges értéke **meg nem engedett mértékben** eltér a szükségestől. Matematikailag felírva a hiba feltétel

$$\Delta x = \left| x_{szüks} - x_{tény} \right| \geq \varepsilon = \Delta x_{eng} = \Delta x_{max} \qquad (2\text{-}1)$$

ahol

$x_{szüks}$- a vizsgált számjellemző adott hibakritériumhoz tartozó szükséges értéke,

$x_{tény}$ – a vizsgált számjellemző tényleges értéke,

$\Delta x_{max} = \varepsilon$ – a szükséges és tényleges érték megengedett maximális eltérése.

Az eltérést akkor tekintjük meg nem engedhetőnek, ha a rendszer célja már nem teljesíthető. Például a rendszercél lehet a biztonság vagy a gazdaságosság. Adott alkatrész esetén alkalmazott túlméretezés az első rendszercél szempontjából megengedhető, míg az utóbbi esetben megengedhetetlen.

Fenti hibaszemlélet alapján a szükséges és tényleges paraméter eltérése csak az eltérés egy meghatározott mértékénél jelent hibát (meghibásodást). A hiba a rendszerkialakítás valamennyi fázisában, így a

- koncepció kialakítása,
- követelmények és feltételek összeállítása,
- konstrukciós tervezés,
- gyártás,
- szerelés,
- vizsgálat,
- üzembe helyezés és
- üzemeltetés (fenntartás)

során egyaránt jelentkezhet. Láthatóan a hibák oka vagy közvetlenül az ember, vagy a gépi berendezések ember által meghatározott működési módja, valamilyen módon tehát az ember követi el. Az emberi hibák elkövetésének lehetséges oka

- hibás cselekvés (amit teszünk, nem helyes), illetve
- mulasztás (nem tesszük meg, amit kellene)

lehet. Ezek mélyebb okai ideiglenes vagy tartós tudatlanság, illetve tévedés (félreértés) lehetnek.

A hibák hatása különböző lehet:

- a nem teljesülő rendszercélok köre szerint
  - egyetlen cél sem teljesül,
  - a célok egy csoportja, vagy
  - csupán egyetlen cél nem teljesül.
- a rendszercél nem-teljesülésének mértéke szerint
  - a rendszercél egyáltalán nem érhető el, vagy
  - a rendszercél időben, teljesítményben csak korlátozottan érhető el.

A hiba, meghibásodás és zavar különbözőképpen definiálható, alapvetően azonban kapcsolatukra a következő mondható:

- **Hiba** alatt értjük az előírt követelmények nem-teljesülését – a hiba ily módon **állapot** (például hibás logikai állapot lehet ilyen).
- A **meghibásodás** egy meghatározott feladat ellátásának megszűnése, tehát ez egy átmenet a hibátlan állapotból a hibásba, vagyis ez egy **esemény,** ami külső hatás nélkül következik be.

- A **zavar** szintén az üzemeltetés során jelentkezik, a rendszertől idegen külső hatásra. A zavar következménye lehet átmeneti (tranziens) vagy tartós (roncsoló) jellegű. Előbbi esetben a zavar megszűnte után a zavar miatti hibás állapot is megszűnik, utóbbiban a zavar megszűnte után sem áll helyre az üzemképes állapot és emberi beavatkozás, javítás szükséges.

A hibák, meghibásodások életciklussal fennálló kapcsolatára nézve mondható, hogy a hibák túlnyomó többsége az üzembe helyezés előtti időszakban jelentkezik, de fellépésük a teljes életciklusban lehetséges. A meghibásodások és zavarok csak az üzembe helyezést követő időszakban jelentkezhetnek. A hibák felismerése természetesen nem feltétlenül következik be az üzembe helyezés előtt, esetenként az üzembe helyezéskor még a berendezésben rejtve vannak, s csak későbbi időpontban ismerhetők fel, sőt esetleg később kerülnek a rendszerbe. Ez alapján megkülönböztethetünk **inherens** (a vizsgált objektumban az üzembe helyezés előtt már meglévő) és **nem inherens** (az üzembe helyezés után keletkező) hibákat. Megállapodás szerűen üzembeállításkor **hibátlan** objektumok megbízhatóságával foglalkozunk csak. A meghibásodások véletlenszerűen később jelentkeznek. Ez érvényes az újonnan üzembe helyezett termék *rejtett hibáira* is, mivel azok csak olyan üzemi körülmények között adódnak, amely a nem **„worst case"** (legkedvezőtlenebb körülményeket figyelembe vevő) tervezést és a gyártási hibákat követő **nem teljes körű tesztelés** miatt maradtak időlegesen rejtve. (Meg kell jegyeznünk, hogy teljes körű tesztelés és minden körülményre kiterjedő worst case tervezés a gyakorlatban rendszerint nem valósítható meg.)

2.2. Meghibásodási és javítási módok

A meghibásodások okai igen sokfélék: oxidáció, túlmelegedés, anyagvándorlás, ESD (=), kémiai átalakulások, diffúziók, kopás stb. lehetnek. A meghibásodások szigorúan véve olyan események, amelyek rögzített időn belül tulajdonképpen nem következhetnének be, ha a rendszer az igénybevételeknek és terheléseknek megfelelően lenne felépítve. Az igénybevételek, terhelések, külső hatások következménye általában nem határozható meg teljesen a tervezés, gyártás idején. Így meghibásodásokkal, illetve zavarokkal feltétlenül számolnunk kell a berendezések élettartama során. Az üzembehelyezés után véletlenszerűen jelentkeznek, bekövetkezésük törvényszerűségeit a későbbiekben részletesebben vizsgáljuk. A meghibáso-

dások végső oka az, hogy a rendszer igénybevételeinek, terhelésének teljeskörű, korrekt figyelembevétele gyakran nem sikerül (vagy nem lehetséges) és az alkatrészek anyagkopás, anyagfogyás, kifáradás stb. miatt törvényszerűen véges élettartammal rendelkeznek.

A meghibásodás leggyakrabban egy hirtelen bekövetkező esemény. Emellett azonban léteznek olyan meghibásodások is, amelyek csak átmeneti jellegűek vagy fokozatosan jelentkeznek, esetleg felismerésük is nehezebb. Például az ún. drift-meghibásodások esetén a vizsgált egység jellemzői lassan változnak és fokozatosan befolyásolják a rendszert, anélkül hogy az adott alkatrész teljes kiesése egyszerre jelentkezne. Hasonlóan nehéz felismerni az időben nem állandó, dinamikus jelleggel fellépő meghibásodásokat, amelyeknél a szükséges és tényleges paraméterértékek csak igen rövid ideig térnek el a megengedettnél nagyobb mértékben.
A jellegzetes meghibásodási módok összefoglalva tehát:

a) **Véletlen időpontban bekövetkező meghibásodások**:

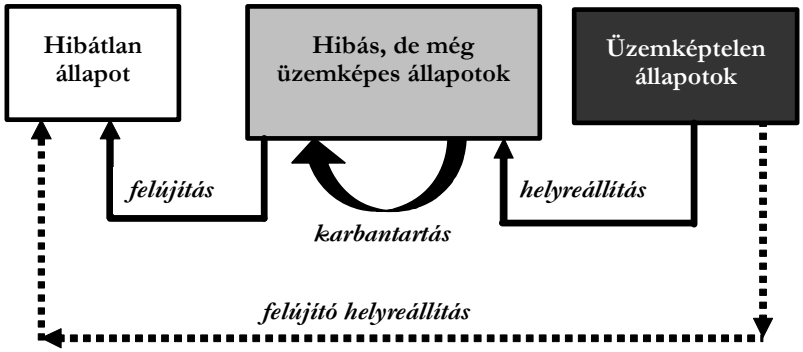
- váratlan (diszkrét) meghibásodás,
- fokozatos (drift jellegű), meghibásodás,
- dinamikus (rövid idejű, váltakozó jellegű, tranziens) átmeneti meghibásodás,
- „katasztrofális" meghibásodás – hirtelen (nem fokozatosan) bekövetkező, végleges és teljes (nem átmeneti jellegű).

b) Ezzel szemben beszélhetünk **másodlagos meghibásodások**ról, ezek korábbi meghibásodások következményei, például egy zárlatossá vált kondenzátor tönkre teszi a hozzá kapcsolódó félvezető eszközt.
A másodlagos meghibásodást **soros rendszerek** esetében figyelmen kívül hagyhatjuk, ha a javítási feltételeket nem befolyásolja számottevően (például mindenképpen ki kell cserélni a teljes meghibásodott egységet). De **redundáns struktúrák** esetében nem egyértelmű a helyzet, mivel egy ilyen esemény és az egységek meghibásodási folyamatai között kapcsolat lehet (az egységek meghibásodása egymástól nem független).

Egy hibátlanul előállított, megfelelően használt objektum esetében a minőségi paraméterek változását és emiatt a megbízhatóságot (sőt a biztonságot) is véletlenszerűen bekövetkező folyamatok jellemzik, amit a környezeti feltételek, a terhelés az objektum robosztussága (ezt a kifejezést szoftverre is használják) döntően befolyásol, de általában valószínűség

számítási módszerek is szükségesek az előrejelzésekhez, becslésekhez, a tapasztalati adatok feldolgozásához.

A javítás eredménye **esemény** – értelem szerűen – a hibák mennyiségének csökkenése. (A javításokra vonatkozó kifejezések sem egységesek a szakirodalomban. Az általunk alkalmazott terminológia kissé leegyszerűsített, 2-1. ábra) Egy javítás lehet adott meghibásodási **eseményt követő** vagy az állapottól független **időszakos.** (Az utóbbi esetben rendszerint tervezetten periodikus). A még üzemképes rendszerben lévő hibák csökkentése a **megelőző karbantartás,** ami szintén lehet eseménykövető, illetve időszakos, (tervszerű megelőző karbantartás). Ha a javítás eredménye a teljesen hibátlan állapot, akkor **felújítás**nak nevezzük. Ha a javítás üzemképtelenből üzemképessé teszi az objektumot, akkor az üzemképesség helyreállításának vagy röviden **helyreállítás**nak nevezzük. A helyreállítás persze lehet adott esetben teljes felújítás is és eseményt követő vagy időszakos is.



2-1. ábra: Javítási módok

Az **eseménykövető** javítás jellegéből adódóan véletlenszerű folyamat, mivel a kiváltó okok is véletlen események. Ezen túl rendszerint a meghibásodás miatti javítások és az ehhez kapcsolódó kiesési idők (hiba felismerés, behatárolás, elhárítás, beállítás, újraindítás stb.) sem pontosan előre adottak, mert véletlenszerű tényezők is befolyásolják.

Összefoglalva: Az öregedés, elhasználódás időpontja is nagy szóródást mutathat, de a zavarok és az emberi hibák, szabotázsok sem a felhasználó számára előre kiszámítható időben következnek be. Egy hibátlanul előállított, megfelelően használt objektum esetében a minőségi paraméterek változását és emiatt a megbízhatóságot is **véletlenszerűen bekövetkező folyamatok** jellemzik. E folyamatokat a környezeti feltételek, a terhelés, az objektum robosztussága döntően befolyásolják. A sok befolyásoló tényező miatt az előrejelzésekhez, becslésekhez, a tapasztalati adatok feldolgozásához általában **valószínűség számítási módszerek** szükségesek.

3. A megbízhatóság jellemzői

3.1. Általános megjegyzések

Az objektum **megbízhatósága** – egyszerűen fogalmazva – **előrejelzés** a minőségre. Ilyen értelemben lehetséges a megbízhatóságot a minőség részének is tekinteni, hiszen ami később is várhatóan jó lesz, az jobb minőségű. Célszerűbb azonban a minőséget a paraméterek egy adott időpontban érvényes értékeihez rendelni, a megbízhatóságot pedig a minőségre vonatkozó, egy későbbi időpontra érvényes **jóslat**nak.

Ez a jóslat azonban felhasználási tapasztalatokon, fizikai és kémiai folyamatok ismeretén alapul és a matematika (valószínűség-számítás) módszereit alkalmazva tudományosan megalapozott. Azért minősítettük mégis jóslatnak, mivel az egyes konkrét objektumokra nem szolgáltathat pontos és biztosan érvényesülő adatokat, de több azonos egyedre vonatkozóan átlagosan érvényes.

Az a kijelentés, hogy egy adott emberi populáció átlagos élettartama 70 év, nyilvánvalóan nem azt jelenti, hogy minden egyede a 70. életévében hal meg, de az adat a nyugdíjbiztosító részére nélkülözhetetlen.

Egyszerűbb termék esetében **a megbízhatóság** (Reliability, Zuverläßigkeit, nagyozsnoszty) **a termék azon képessége, hogy megfelel az alkalmazási célnak adott környezeti feltételek között, adott időtartamra.**

Meg kell rögtön jegyeznünk, hogy az előzőekben szereplő **idő** helyett egyes esetekben más **független változónak** tekintett paraméter szerinti analízis, illetve előrejelzés alkalmazása indokolt. A ciklikusan működtetett objektum (például egy kapcsoló) esetében a **ciklusszám,** egy jármű esetében a **megtett úthossz** veendő számításba az idő helyett, esetleg az idő mellett. Egy merevlemezes tárolónál az üzemidőn kívül a **ki- és bekapcsolások száma,** egy programozható memória esetében a törlési-programozási **műveletek száma** mérvadó.

A megbízhatóságra adott meghatározás minőségi definíciónak tekinthető, de mérnöki alkalmazások szempontjából igen fontos, hogy azt számszerűen is jellemezni tudjuk. Ha feltételezzük, hogy nagyszámú ilyen vizsgált egységünk van, amelyek azonos üzemi feltételek között egyidejűleg mű-

ködnek, akkor ezek – amennyiben a hibák véletlenszerűen jelentkeznek – különböző T üzemidők után kerülnek a működőképes állapotból a meghibásodott állapotba. A meghibásodások időbeli alakulásának számszerű jellemzésére különböző megbízhatósági paraméterek határozhatók meg

E paraméterek megadása általában a következő adatokkal történik:

- számérték,
- mértékegység,
- meghibásodási feltételek,
- meghibásodást befolyásoló tényezők,
- vizsgált időtartam.

A biztonság és a megbízhatóság értékelésekor a termék általános érvényű, objektív összehasonlíthatóságára módot adó, lehetőleg számszerű jellemzők meghatározására törekszünk. A megbízhatóság számszerűsítése történhet determinisztikus és sztochasztikus jellemzőkkel.

A **determinisztikus** jellegű biztonsági és megbízhatósági tulajdonságokhoz azonban nem mindig rendelhetők számszerű paraméterek.

A **sztochasztikus** jelleggel érvényesülő folyamatokhoz számszerű paraméterek, függvények rendelhetők, de ezek viszont egy-egy objektumra statisztikus jelleggel csak közelítő becslésnek tekintendők, amelyek az adott termék típusra *átlagosan* érvényesek.

Vizsgáljuk meg e jellemzőket részletesebben!

3.2. Determinisztikus jellemzők

A leggyakrabban használt determinisztikus jellemzők :

- robosztusság, (bolond-biztos, fullproof, idiotenfest)
- javíthatóság (maintability), cserélhetőség, bonthatóság
- sebezhetőség (vulnerability).

A determinisztikus jellemzők az adott objektum típus minden elemére egyformán érvényesek. Az ilyen jellemzők olyan mértékben kötődnek a konkrét alkalmazáshoz és a megvalósítás konstrukciós megoldásához, hogy általános jelleggel nem értékelhetők, ezért nem tekinthetők az adott típusú objektum általános jellemzőjének. A determinisztikus jellegű tulajdonságok viszont olyan jelentős mértékben befolyásolhatják a biztonságot és a megbízhatóságot, hogy feltétlenül **figyelembe** kell venni őket, (ha **számításba** venni nem is mindig lehet). A robosztusság például ideális

felhasználó esetében nem hoz előnyt, szakszerűtlen, figyelmetlen alkalmazónál viszont jelentősen növelheti a várható élettartamot. A javíthatóságot pedig erősen befolyásolja a karbantartók képzettsége, felszereltsége.

A determinisztikus jellemzőkhöz kapcsolódó **meghibásodások** sem egy adott előre meghatározható időpontban következnek be, hiszen kezelési anomáliákhoz vagy esetleg terrorakciókhoz kötődnek és így csak **véletlen folyamatként** vehetők figyelembe.

Vizsgáljuk részletesebben a leggyakoribb determinisztikus jellemzőket:

3.2.1. Robosztusság

A robosztusság az olyan, általában nem szándékos üzemeltetői (főleg emberi) hibák tűrését jelenti, amelyek az objektum eredeti működési tartományának túllépésekor keletkeznek. Ilyen a hibás beállítás, a figyelmetlen, szakszerűtlen kezelés stb.
Példák a robosztusság növelésére:

- A műszer, rádióvevő, óra stb. beállító forgató gombjához kapcsolódó mechanikus szerkezet a végállás elérésekor egy csúszó tengelykapcsoló nyomatékhatárolása révén megakadályozza a túlcsavarásból eredő roncsolódást.
- A generátor, a tápegység túlterhelés védett.
- A mérőműszer, erősítő, végrehajtó egység túlvezérlés védett.
- A szoftver a hibásnak tűnő adat és utasítás előfordulásakor figyelmeztető jelzést ad, nem hajtja végre a műveletet alkalmazói megerősítés nélkül. (Valóban törölni akarja valamennyi filet?)

3.2.2. Javíthatóság

A javíthatóság és az ezt lehetővé tevő mechanikai és villamos *bonthatóság, cserélhetőség, visszaállíthatóság* szintén fontos megbízhatósági jellemzők. Ennél a tulajdonságnál hangsúlyt kap a helyreállítás költsége (érdemes-e javítani, a helyreállítás eredménye tökéletes állapot lesz-e stb.).

A példákból is látható, hogy fontos, de értékében bizonytalan, nehezen általánosítható és számszerűsíthető tulajdonságokról van szó. A robosztusság például ideális felhasználó esetében nem hoz előnyt, szakszerűtlen alkalmazónál viszont jelentősen növelheti a várható élettartamot. A javíthatóságot pedig erősen befolyásolja a karbantartók képzettsége, a tartalékkészletek megléte.

3.2.3. Sebezhetőség

A sebezhetőség a vizsgált objektumnak az a tulajdonsága, amely megadja, milyen minimális mértékű adott fajtájú szándékos hiba okozással (szabotázs, háborús vagy terror cselekmény) tehető az objektum működésképtelenné, illetve milyen mértékű az a maximális károkozás, ami még nem eredményez üzemképtelenséget.

Egy példával illusztrálva: tekintsünk egy informatikai hálózatot üzemképesnek, ha (adott időbeli, kapacitásbeli korlátozással) valamennyi csatlakozó partner (előfizető) képes bármelyik másikkal kapcsolatot létesíteni. Ha ez a hálózat kétirányú forgalomra képes egyvonalas felépítésű, akkor egyetlen összeköttetést elvágva üzemképtelenné válik, de ha gyűrűs struktúrájú, akkor legalább két összeköttetést kell ehhez elvágni. A kerülő utakat is tartalmazó szövevényes hálózat még kevésbé sebezhető egy-egy összeköttetés elrontásával. A bonyolult hálózatok sebezhetőségének analízise nem olyan triviális, mint a fenti példa. A gráfelmélet módszereit alkalmazzák és ekkor a sebezhetőséget számszerűsíthető paraméter is jellemezheti. Megjegyzendő, hogy utóbbi eredmények a véletlen meghibásodási folyamatok esetén is hasznosíthatók.

3.3. Sztochasztikus jellemzők

3.3.1. Általános megjegyzések

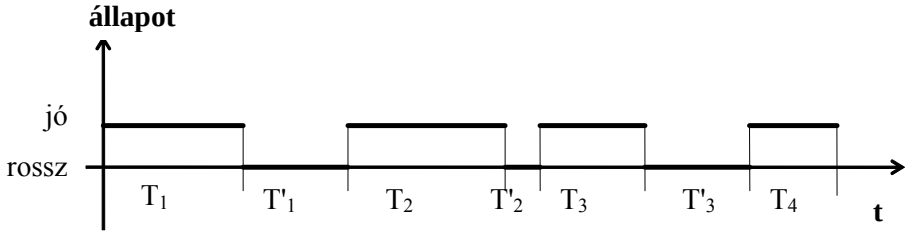
A megbízhatóság sztochasztikus jellemzői a meghibásodások gyakoriságára, sűrűségére (sebességére), illetve a vizsgált meghibásodási folyamat időértékeire vonatkozhatnak:

- egyes minőségi paraméterek (a meghibásodási folyamat állapotvalószínűségeinek) várható értékei,
  - megbízhatósági függvény
  - meghibásodási függvény
- a meghibásodási folyamat sebességére jellemző paraméterek:
  - meghibásodási sűrűségfüggvénye,
  - meghibásodási tényező,
- a meghibásodási folyamathoz tartozó várható (idő)tartamok:
  - első meghibásodásig várható jó működési idő
  - átlagos jó működési idő,
  - üzemképtelen állapotban eltöltött idők átlaga,

- javítható rendszer meghibásodási folyamatának hatásfok jellegű jellemzői:
  - üzemkészség (készenléti tényező),
  - üzemképtelenség.

A sztochasztikus paraméterek különböző módszerekkel határozhatók meg. A meghibásodási folyamatra vonatkozó paramétereket egy nagyobb alkatrész készlet meghibásodásainak elemzésével határozhatjuk meg. Példaként tekintsük azt az esetet, amikor $\mathbf{N_0}$ db alkatrész vizsgálatát végezzük, feltételezve, hogy a vizsgálat kezdeti időpontjában (t=0) valamennyi alkatrész jó. A használat során különböző időpontokban különböző mennyiségű alkatrész hibásodik meg, a meghibásodott alkatrészek számát meghatározott időközönként feljegyezzük. Jelöljük **N(t)**-vel a t időpontban még jó alkatrészek számát. A folyamatra vonatkozó adatok alapján meghatározhatjuk adott Δt idő alatt meghibásodott alkatrészek számát is, amiből aztán az egyes sztochasztikus jellemzőket meghatározhatjuk.

A véletlen folyamatokra jellemező időtartamok értelmezését a következő modell segíti. Legyen egy termék a t=0 időpontban üzembe helyezve előírásosan jó állapotban. T_1 ideig jól működik, ekkor meghibásodik (failure, Ausfall, otkáz), de megjavítják. A hiba miatt T'_1 időtartamra üzemképtelen, de utána T_2 ideig megint jó, majd T'_2 alatt ismét rossz stb. Az elmondottakat a 3-1. ábra idődiagramja szemlélteti.



3-1. ábra: Meghibásodási folyamat idődiagramja

3.3.2. Állapotvalószínűségek, mint megbízhatósági jellemzők

3.3.2.1. Meghibásodási függvény

A **meghibásodási függvény** valószínűség-értékét ilyen esetben a meghibásodott alkatrészek relatív mennyiségével közelíthetjük. Ezek alapján a meghibásodási függvény:

$$\hat{F}(t) = \frac{N_0 - N(t)}{N_0} \tag{3-1}$$

ahol az összefüggés számlálója ellenőrizhető módon a **t** időpontig meghibásodott alkatrészek számát jelenti. E definíció alapján ez a függvény a meghibásodások eloszlásfüggvényének tekinthető.

3.3.2.2. Megbízhatósági függvény

A **megbízhatósági függvény** empirikus értéke hasonlóan a t időpontot túl élő alkatrészek relatív mennyiségeként:

$$\hat{R}(t) = \frac{N(t)}{N_0} \tag{3-2}$$

A kapott két összefüggés összegét képezve ellenőrizhető a két függvény között eseményalgebrailag fennálló 1-es komplemens tulajdonság teljesülése (vizsgált elem a t időpontban vagy hibás, vagy még jó, tehát a két valószínűség összege természetesen kiadja a teljes valószínűséget):

$$\hat{F}(t) + \hat{R}(t) = \frac{N_0 - N(t)}{N_0} + \frac{N(t)}{N_0} = \frac{N_0}{N_0} = 1 \tag{3-3}$$

3.3.3. Meghibásodások sebességére jellemző paraméterek

3.3.3.1. A meghibásodások sűrűségfüggvénye

Valamely sebesség-jellegű paraméter számértékét úgy képezhetjük, hogy az adott időintervallumban meghibásodott alkatrészek relatív számának egységnyi időre eső részét képezzük. A meghibásodások időbeli alakulására vonatkozó jellemző meghatározása esetén a meghibásodások relatív mérőszámát első esetben a kezdeti jó alkatrészek $\mathbf{N_0}$ számára vonatkozóan számítjuk és a paramétert jelöljük $\hat{f}(t)$ módon vagyis

$$\hat{f}(t) = \frac{n_i}{N_0 \cdot \Delta t} \tag{3-4}$$

ahol az $\mathbf{n_i}$ az i-ik időintervallumban jelentkező meghibásodásokat jelenti, ennek meghatározási módja:

$$n_i = N(t) - N(t + \Delta t) \tag{3-5}$$

Ennek figyelembevételével:

$$\hat{f}(t)=\frac{N(t)-N(t+\Delta t)}{N_0\cdot\Delta t} \tag{3-6}$$

A kapott eredmény kis átalakításával belátható, hogy ez a paraméter a meghibásodási függvény növekményével áll szoros kapcsolatban:

$$\hat{f}(t)=\frac{N_0-N(t+\Delta t)-\left[N_0-N(t)\right]}{N_0\cdot\Delta t}=\frac{\hat{F}(t+\Delta t)-\hat{F}(t)}{\Delta t}=\frac{\Delta\hat{F}}{\Delta t} \tag{3-7}$$

vagyis az így meghatározott paramétert joggal neveztük a meghibásodások sűrűségfüggvényének.

Itt is ellenőrizhető, hogy a meghibásodások sűrűségfüggvénye a meghibásodási függvény idő szerinti deriváltjával egyezik, mint ahogy azt a később szereplő (4-15) képlet mutatja.

3.3.3.2. Meghibásodási tényező (ráta)

A meghibásodási tényező (FR = Failure Rate, Ausfallrate, intyenszívnoszty otkázov), mint másik lehetséges sebességparaméter empirikus értékét az előzőekhez rendkívül hasonló módon kapjuk, csak a meghibásodások relatív számának képzésénél az időszakhoz tartozó jó alkatrészek számát tekintjük viszonyítási alapnak. Belátható, hogy a számértékek ugyan függnek attól, hogy az időszak melyik pontjára érvényes értékhez viszonyítunk, de az időbeli alakulás reális felméréséhez elegendő, hogy az időszak ugyanazon pontjához tartozó értékekkel számoljunk. Önkényesen tehát a mindenkori vizsgált időszak elején még jó alkatrész-számot vehetjük viszonyítási alapként. Ezzel

$$\hat{\lambda}(t)=\frac{n_i}{N(t)\cdot\Delta t}=\frac{N(t)-N(t+\Delta t)}{N(t)\cdot\Delta t} \tag{3-8}$$

A többi eddig szereplő megbízhatósági számjellemzővel fennálló matematikai kapcsolat ezen összefüggés kis algebrai átalakításával szintén belátható. A számlálót és nevezőt egyaránt $1/N_0$ tényezővel bővítve a későbbiekben ismertetett és matematikailag bizonyítható összefüggéseket kapjuk:

$$\hat{\lambda}(t)=\frac{N(t)-N(t+\Delta t)}{N(t)\cdot\Delta t}=\frac{\frac{N(t)-N(t+\Delta t)}{N_0\cdot\Delta t}}{\frac{N(t)}{N_0}}=\frac{\frac{\Delta\hat{F}}{\Delta t}}{\hat{R}(t)}=\frac{\hat{F}'(t)}{\hat{R}(t)}=-\frac{\hat{R}'(t)}{\hat{R}(t)} \quad (3\text{-}9)$$

3.3.4. A meghibásodási folyamathoz tartozó várható (idő)tartamok

3.3.4.1. Az első meghibásodásig várható jó működési idő (MTTF)

Az MTTF (= **M**ean **T**ime **T**o **F**ailure) jellemző a 3-1. ábra szerinti T_1 átlagértéke (egyes szakkönyvekben, cikkekben az első meghibásodás hangsúlyozására, vagyis ha a meghibásodásokat javítások követik) MTTFF (= **M**ean **T**ime **T**o **F**irst **F**ailure) rövidítés is szokásos:

$$T_F = M\{T_1\} \qquad (=MTTF) \quad (3\text{-}10)$$

Ez az átlagérték eredetileg több (sok) azonos típusú termék alkalmazási tapasztalataként értelmezett, a gyakorlatban azonban rendszerint előre jelzett számított érték.

3.3.4.2. Az átlagos jó idő (MUT)

A MUT = **M**ean **U**p **T**ime paraméter a 3-1. ábra szerinti T_i idők átlagértéke i = 1, 2, 3...

$$T_U = M\{T_i\} \quad (3\text{-}11)$$

Ez az érték egyetlen objektum tartós alkalmazásának szerviz statisztikájából, több (sok) meghibásodási-javítási eseményhez tartozó jó idők átlagaként értelmezett, de lehetséges több azonos típusú objektumra vonatkozóan is számítani. Gyakorlatilag a két módszertől azonos eredményt várhatunk, ha a javítás egyformán az előírásos jó állapotot eredményezi és a termék nem öregszik, nem használódik közben el. Matematikailag ez az egyezés feltételnek tekintendő.

A $\mathbf{T_F}$ és $\mathbf{T_U}$ értéke is egyenlő, ha az előző feltételek érvényesek. Egyébként ilyenkor a leggyakrabban – nem egészen korrekt módon MTBF-t (= **M**ean **T**ime **B**etween **F**ailures) írnak.

A **jó** idő lehet működő (operating), készenléti állapotban lévő (stand by), illetve nem üzemelő de üzemképes (free).

3.3.4.3. Az üzemképtelen állapotban töltött idők átlaga (MDT)

Az MDT = **M**ean **D**own **T**ime paraméter a 3-1. ábra szerinti T_i' idők átlagértéke:

$$T_D = M\{T_i'\} \tag{3-12}$$

Erre az átlagolásra is vonatkoztathatók a $\mathbf{T_U}$ kapcsán elmondottak.
A $\mathbf{T_D}$ a következő részidőkből tevődhet össze:

- a meghibásodás pillanatától annak észleléséig :
  MFDT = Mean Failure Detection Time
- a hiba javításához szükséges idő: **MTTR = Mean Time To Repair** (mely az alábbi összetevőkből áll:
  - o várakozás a hiba elhárítására (pótalkatrészre, a szerviz szerelőre)
  - o a hiba kijavítása, a hibás elemek cseréje
  - o vizsgálat, mérések, próba,
  - o újraindítás.

Az utóbbi két részidőt a $\mathbf{T_D}$ helyett a $\mathbf{T_U}$-hoz számítják, ha nem a felhasználó szempontjait veszik figyelembe, hisz ezen műveletek idején a berendezés már működik, csak még nem áll a felhasználó rendelkezésére.

3.3.5. Javítható rendszerek megbízhatósági jellemzői

3.3.5.1. Tartós üzemkészség

A tartós üzemkészséget (amelyet készenléti tényezőnek is neveznek, = availability, Dauerverfügbarkeit, gatovnoszty), a következőképpen határozhatjuk meg:

$$K = \frac{T_U}{T_U + T_D} \tag{3-13}$$

Tehát valóban hatásfok jellegű mennyiség, azt mutatja meg, hogy a teljes üzemidő mekkora részében használható az adott rendszer, mennyire áll a felhasználó rendelkezésére (ezért számos irodalomban rendelkezésre állásnak is hívják ezt a jellemzőt).

3.3.5.2. Tartós üzemképtelenség

A fenti jellemző komplemens valószínűsége (Dauernichtverfügbarkeit), az angolszász irodalomban **DTR** (= **D**own **T**ime **R**atio) módon jelölve:

$$K_D = \frac{T_D}{T_U + T_D} = 1 - K \tag{3-14}$$

A valóságban $K_D \ll 1$. (Például $K_D = 10^{-3}$ azt jelenti, hogy az idő egy ezrelékében nem áll rendelkezésre az objektum hosszú idő átlagában. K = 0,999 ugyanezt jelenti, így a kettő közül csak az egyiket van értelme megadni és csak szokás kérdése, melyik szerepeljen a termék specifikációjában.)

3.3.5.3. A javítási, hibaelhárítási tényező (ráta)

A javítási intenzitás $\mu(t)$ a meghibásodási tényezőhöz hasonlóan függvénnyel definiálható. Tekintsük most az egyszerűség kedvéért az intenzitást az időben állandó tényezőnek, azaz rátának, ami a T_D idő reciprokával egyező:

$$\mu(t) = \mu = \frac{1}{T_D} \tag{3-15}$$

Ez az összefüggés azonban csak közelítő jellegű! Az okokkal a továbbiakban foglalkozunk, a korrektebb függvény számításba vétele később tárgyalt bonyolultabb modell apparátusát igényli. Ezért a közelítést a gyakorlatban nem ritkán kényszerből alkalmazzák.

3.3.5.4. A megelőző karbantartások (TMK) közötti üzemidő (MTTPM)

A paraméter jelentése az angolszász irodalomban **MTTPM** (= **M**ean **T**ime **T**o **P**reventive **M**aintenance)

4. A minőség és a megbízhatóság kapcsolata

4.1. A minőség és megbízhatóság matematikai kapcsolata

Az objektum minőségi jellemzői véges számú (n) paraméterrel leírhatók:

$$q_1(t), q_2(t), q_3(t), \ldots, q_i(t), \ldots, q_n(t).$$

Ezek a paraméterek általában nem állandó értékűek, hanem időben változók, vektorba rendezve:

$$\underline{Q}^T(t) = [q_1(t), q_2(t), q_3(t), \ldots, q_i(t), \ldots, q_n(t)] \qquad (4\text{-}1)$$

Ez a $Q^T(t)$ adja meg az objektum minőségét adott t időpontban. Bár a $q_i(t)$ paraméterek az objektum korával, igénybevételével függésben lehetnek, de ez a függés csak statisztikusan érvényesül. Pontosan nem is mindig ismerhető és sok véletlen hatás befolyásolja, ezért általános esetben $Q^T(t)$-t az időben **véletlenszerűen változónak** kell tekintenünk.

A $\mathbf{Q^T(t)}$ vektor az adott objektumra valamennyi lehetséges paramétert tartalmazó **Ω „eseménytérben”** egy **n** dimenziós görbét ír le az idő függvényében, ez a görbe tulajdonképpen az objektum „története”, ami ilyen részletesen gyakorlatilag érdektelen a megbízhatósági analízis szempontjából. Célszerűbb $Q^T(t)$ lehetséges teljes értékkészletét olyan diszjunkt részhalmazokra felosztani, amelyek a használhatóság szempontjából egyenértékű paramétereket tartalmaznak. (Ezeknek a résztartományoknak nem kell feltétlenül folytonosan összefüggőknek lenniük.) Mivel közömbös $\mathbf{Q^T(t)}$ pontos értéke, elegendő annak ismerete, hogy ez a minőségi vektor éppen melyik tartományon belül van, hiszen azon belül ekvivalensnek tekintjük a paraméterértékeket.

Legyen **Ω** a $\mathbf{Q^T(t)}$ valamennyi lehetséges értékét tartalmazó n-dimenziós állapottér:

$$\underline{Q}^T(t) \in \Omega \qquad (4\text{-}2)$$

amelyet m véges számú diszjunkt (egymást kölcsönösen kizáró) résztartományra osztunk, ezek a tartományok:

$$Z_1, Z_2, Z_3, \ldots, Z_m,$$

Ezek a tartományok egymást kölcsönösen kizárják, vagyis $Z_i \cap Z_j = \Phi$ üres halmaz , ha i ≠ j és

$$\bigcup_{i=1}^{m} Z_i = \Omega \tag{4-3}$$

azaz a résztartományok uniója lefedi a teljes állapotteret.

Azt, hogy az objektum t időpontban éppen az i-edik tartományban (állapotban) van, leírhatjuk egyszerűbben is, ha bevezetünk egy **x(t)** folytonos idejű, diszkrét értékkészletű változót, ami **m** állapot esetében egy adott t időben 1, 2, 3, … m pozitív egész számok közül vehet fel értéket. Ez a szám az objektum **állapot index**e, így x(t)=i azt jelenti, hogy az objektum az i-edik állapotban (tartományban) van.

$$x(t) = i, \quad \text{ha} \quad Q^T(t) \in Z_i \tag{4-4}$$

Legyen az állapotok (paraméter tartományok) indexelése önkényesen rendezett így:

$\mathbf{Z_1}$ a tökéletes, **előírásos** állapothoz tartozó tartomány,
$\mathbf{Z_2, Z_3, \ldots Z_h}$ a **hibás**, de még üzemképes állapotokhoz tartozó,
$\mathbf{Z_{h+1}, Z_{h+2}, \ldots Z_m}$ pedig az **üzemképtelen** állapotokhoz tartozó tartományokat jelenti.

Ha tehát **x(t) ≤ h,** akkor **üzemképes** az objektum,
ha pedig **x(t) > h,** akkor **üzemképtelen**.

A legegyszerűbb esetekben (alkatrészek, kevés elemből felépülő, egy funkciójú készülékek) elegendő csak két állapotcsoportot értelmezni:
üzemképes (up):

$$Z_U = \bigcup_{i=1}^{h} Z_i \qquad \text{azaz} \quad x(t) \le h \tag{4-5}$$

és **üzemképtelen(down):**

$$Z_D = \bigcup_{i=h+1}^{m} Z_i \qquad \text{azaz} \quad x(t) > h \tag{4-6}$$

Persze így is igaz, hogy

$$Z_U \bigcup Z_D = \Omega, \text{ és } Z_U \bigcap Z_D = \Phi \tag{4-7}$$

Ilyen egyszerű esetben az **x** állapot index csak kétféle értéket vehet fel. A Boole algebra, illetve a bináris számrendszer alkalmazhatósága érdekében **x** két lehetséges értékének (önkényesen) a **0**-t és az **1**-t választjuk, célszerűen most **x=1** a jó, $\mathbf{Z}_U$ állapothoz és az előzőekben nem használt **x=0** a rossz, $\mathbf{Z}_D$ állapothoz rendelendő.

Bonyolult objektum esetében is használatos lehet ez a megbízhatósági függvények és paraméterek szempontjából igen egyszerű, kétállapotú modell, azonban a közbenső számítások többségében a többállapotú modellre van szükség, hogy

- a hibás, de még üzemképes állapotokban az egyes funkciók rendelkezésre állását külön is meghatározhassuk,
- az üzemképtelen állapotokban figyelembe vehessük a könnyen, illetve a nehezen javítható és a javíthatatlan állapotok közötti különbséget.

A számítások végeredménye ezután a kétállapotú modellre vonatkoztatva is megadható, így például a $\mathbf{Z}_U$ -hoz rendelt valószínűség a $\mathbf{Z}_1 \ldots \mathbf{Z}_h$ állapotok valószínűségeinek összege. Végül is a számítási modell két, vagy többállapotú változatától függetlenül értelmezendők az alábbi összefüggések:

A jó állapotban való tartózkodás valószínűsége az objektum **üzemkészség**e (rendelkezésre állása = dependability, Verfügbarkeit, gatovnoszty):

$$d(t) = \Pr\left\{ Q(t) \in Z_U \right\} \tag{4-8}$$

Ez tehát annak valószínűsége, hogy az objektum jó, mert nem hibásodott még meg, illetve ha meghibásodott korábban, akkor már helyreállították és a t időpontban üzemképes.

Amennyiben a meghibásodás esetén nem javítják meg az objektumot, mert nem érdemes vagy nem is javítható, akkor a hibamentes működés valószínűségét adják meg. Ezt gyakran – de nem korrekt módon – egyszerűen megbízhatóságnak is nevezik (reliability, Ausfallfreiheit, bezotkáznoszty):

$$r(t) = \Pr\left\{ Q(t') \in Z_U \right\} \quad \forall\, t' \le t \tag{4-9}$$

Persze $d(t) \mapsto r(t)$, ha a javítási idő minden határon túl nő.

A d(t) és az r(t) függvényeket csak a pozitív időtartományra értelmezzük

$$d(t) \equiv 0 \quad \text{és} \quad r(t) \equiv 0, \quad \text{ha} \quad t < 0 \tag{4-10}$$

A **t = 0** időpontban viszont tökéletesen hibamentesnek tekintjük az objektumot:

$$d(0)=1 \quad \text{és} \quad r(0)=1 \tag{4-11}$$

Ha az idő minden határon túl nő, a **d(t)** egy pozitív határértékhez tart:

$$d(t)\mapsto K, \quad \text{ha} \quad t\mapsto\infty. \tag{4-12}$$

Ez a K határérték a készenléti tényező (availability, Dauerverfügbarkeit, gatovnoszty). Bizonyítható, hogy ez megegyezik a korábbi, definíciónak tekintett összefüggésből adódó készenléti tényezővel.

K értéke nullánál nagyobb, ha minden egyes meghibásodást követően javítják az objektumot. Amennyiben az egyes jó működési idők átlaga, valamint a hiba miatti kiesési idők (üzemképtelen, rossz állapot, hibaelhárítás, újraindítás stb.) átlaga az idő múltával stabilitást mutat, K állandó értékű.

A gyakorlatban K jó közelítése d(t)-nek, mivel utóbbi aszimptotikusan, kis tranziens idő alatt tart a határértékhez, így az értéke rövid időn belül kis hibával és biztonsággal [mivel mindig K < d(t)] helyettesítheti az időfüggvényt.

Feltételezzük viszont, hogy semmi sem tart örökké, tehát ha nem javítják az objektumot:

$$r(t)\mapsto 0, \quad \text{ha} \quad t\mapsto\infty. \tag{4-13}$$

Ha F(t) az r(t) komplemens valószínűsége (meghibásodási függvény):

$$F(t)=1-r(t), \quad \text{és így} \quad F(0)=0 \quad \text{valamint} \quad F(\infty)=1, \tag{4-14}$$

akkor ezekből és abból a kikötésből, hogy egy ilyen magára hagyott objektum monoton nem javul, adódik, hogy az F(t) meghibásodási függvény matematikailag eloszlásfüggvény, a „meghibásodások eloszlásfüggvénye" elnevezés is szokásos.

Az F(t) deriválható és létezik az f(t) sűrűségfüggvény:

$$f(t)=\frac{dF(t)}{dt}=-\frac{dr(t)}{dt} \tag{4-15}$$

A fenti önkényes, de célszerű megállapodásoktól csak kivételes esetben térnek el, tehát ezeket alapértelmezésnek kell venni.

A meghibásodási tényező a korábbi empirikus meghatározási móddal egyezően matematikailag az alábbi függvénnyel definiálható. Ha a meghibásodást követően nincs javítás, akkor:

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{P_r\left[t < T_1 \le (t + \Delta t) \middle| T_1 > t\right]}{\Delta t} = -\frac{R'(t)}{R(t)} \qquad (4\text{-}16)$$

Szóban megfogalmazva: λ annak az eseménynek a feltételes valószínűsége, hogy az objektum egységnyi (Δt) idő alatt megy tönkre egy adott t idő után, feltéve, hogy addig jó volt és az időegység (Δt) igen kicsi. Erősen leegyszerűsítve ez az „elromlás", a meghibásodás **sebesség**e.

Az empirikus meghatározás alapján kapott (3-9) összefüggéssel való egyezés igazolására vizsgáljuk meg annak a valószínűségét, hogy egy **t** ideig már hibátlanul működött alkatrész egy további (t, t_1) időszakban nem hibásodik meg. Jelöljük ezt a valószínűséget $P(t,t_1)$ módon. Jelentse A illetve B azt az eseményt, hogy az alkatrész hibamentesen működik a (0,t) illetve a (t,t1) időintervallumban. Ekkor a keresett valószínűség a

$$P(t, t_1) = P\{A|B\} = \frac{P\{A \cdot B\}}{P\{A\}}$$

feltételes valószínűség. Az A·B együttes esemény azonban az alkatrésznek a teljes $(0,t_1)$ időintervallumban való hibamentes működését jelenti, ezért

$$P(t, t_1) = \frac{R(t_1)}{R(t)}.$$

Ebből a (t, t_1) időintervallumban való meghibásodás valószínűsége ennek 1-es komplemenseként adódik:

$$F(t, t_1) = 1 - P(t, t_1) = \frac{R(t) - R(t_1)}{R(t)}.$$

Ha a t_1 időpontot a t viszonylag kis környezetében választjuk meg $t_1 = t + \Delta t$ módon, akkor

$$F(t, t + \Delta t) = \frac{R(t) - R(t + \Delta t)}{R(t)} = -\frac{\Delta R}{R}.$$

Ha a Δt értékét 0-hoz közelítjük, akkor

$$F(t, t+\Delta t) = -\frac{\Delta R}{R(t)} = -\frac{\frac{\Delta R}{\Delta t}\cdot \Delta t}{R(t)} = -\frac{R'(t)}{R(t)}\cdot \Delta t + o(\Delta t),$$

vagy ha bevezetjük a

$$\lambda(t) = -\frac{R'(t)}{R(t)}$$

jelölést, akkor kis Δt értékekre tényleg azt kapjuk, hogy

$$\lambda(t) \approx \frac{F(t, t+\Delta t)}{\Delta t},$$

ahogy az a (4-16) egyenletben szerepelt.

A $\lambda(t)$ időfüggésével a 4.3. fejezetben foglalkozunk, azonban az elektronikus alkatrészek döntő többségének a meghibásodási tényezője **állandó az időben** és ez esetben **rátá**ként (konstans paraméterként) adható meg, amely adat a kereskedelmi forgalomban lévő termékek (alkatrészek) katalógusában is megtalálható. Ennek a ténynek igen nagy a gyakorlati jelentősége, ezért a paraméterek és függvények közötti összefüggések ismertetését követően erre a kérdésre részletesen vissza kell térnünk.

4.2. A megbízhatósági jellemzőkre vonatkozó alapösszefüggések

Az eddig megismert sztochasztikus jellemzők között matematikai összefüggések vannak. A meghibásodási tényező definíciójából következik a megbízhatóság elmélet egyik legalapvetőbb általános összefüggése:

$$R(t) = \exp\left[-\int_0^t \lambda(\tau)\cdot d\tau\right] \qquad (4\text{-}17)$$

Bizonyítás:

A korábbi λ-ra vonatkozó (4-16) képlet alapján

$$\lambda(t) = -\frac{dR(t)}{dt} \cdot \frac{1}{R(t)} \tag{4-18}$$

Ezt szétválasztva és integrálva

$$\int_0^t \frac{dR(\tau)}{R(\tau)} = -\int_0^t \lambda(\tau) \cdot d\tau \tag{4-19}$$

és az integrálást elvégezve:

$$\ln R(t) = -\int_0^t \lambda(\tau) \cdot d\tau + c \tag{4-20}$$

ahol **c=0**, mivel **r(0)=1** és $t \geq 0$. Így **r(t)**-re valóban a fenti összefüggést kapjuk.

Az első meghibásodásig várható jó idő (MTTF) pedig:

$$T_F = \int_0^\infty R(t) \cdot dt \tag{4-21}$$

Ez a megbízhatóság elmélet második alapvető általános összefüggése.

Bizonyítás:

A $\mathbf{T_F}$ definíciója alapján:

$$T_F = M\{T_1\} = \int_{-\infty}^{\infty} t \cdot f(t) \cdot dt = -\int_0^\infty t \cdot \frac{dR}{dt} \cdot dt \tag{4-22}$$

ahol $f(t) = -\frac{d\,R(t)}{dt}$, mivel $F(t) = 1 - R(t)$ eloszlásfüggvény, aminek **f(t)** sűrűségfüggvény a deriváltja. A parciális integrálás érdekében, a szorzatfüggvények deriválási szabálya alapján írható, hogy:

$$t \cdot dR = d(t \cdot R) - R \cdot dt \tag{4-23}$$

Az **R(t)**-re vonatkozó korábban rögzített feltételek szerint:

$$R(t) = 0 \;\forall\; t < 0,\; F(0) = 0,\; \text{és } F(\infty) = 1 \tag{4-24}$$

ezért $\left[t \cdot R\right]_0^{\infty} = 0$ adódik (ugyanis joggal tételezzük fel, hogy ha $t \to \infty$, akkor $\lambda(t)$ az időben növekvő, esetleg állandónak tekinthető, de semmiképpen nem csökken).

Igen fontos gyakorlati eset, hogy ha $\lambda(t) = \lambda$ **állandó értékű,** akkor a (4-17) alapján:

$$r(t) = e^{-\lambda \cdot t} \tag{4-25}$$

A (4-25) alapján az exponenciális függvényt integrálva kapjuk, hogy

$$T_F = \int_0^{\infty} e^{-\lambda \cdot t} \cdot dt = \frac{1}{-\lambda} \cdot \left[e^{-\lambda \cdot t}\right]_0^{\infty} = \frac{1}{\lambda} \tag{4-26}$$

(Két utóbbi összefüggés természetesen csak akkor érvényes, ha λ állandó értékű.)

4-1. példa

Egy termék meghibásodási tényezője: $\lambda = 10^{-6}$ /óra. Egy évig üzemeltetve mennyire csökken a megbízhatósága?

Megoldás:

t = 1 év = 8760 óra

$$r(t) = e^{-\lambda \cdot t} \approx 1 - \lambda \cdot t = 1 - 8,76 \cdot 10^{-3} \approx 99\%$$

ugyanis $e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots \approx 1 + x$ ha $|x| << 1$

Az előzőekben matematikai levezetéssel megismertük a megbízhatósági számjellemzők között fennálló legalapvetőbb összefüggéseket. E jellemzők egy csoportja különös jelentőségű az összefüggések szempontjából. A megbízhatósági-, meghibásodási-függvény, a meghibásodások sűrűségfüggvénye és a meghibásodási tényező olyan kapcsolatban állnak egymással, hogy egyetlen ismeretében a másik három mindig meghatározható. Esetről esetre nem adjuk meg az összefüggések matematikai igazolását, de táblázatosan összefoglalva közöljük azokat (lásd a 4-1. táblázatot). A táblázatban szereplő összefüggések magyarázzák, hogy bizonyos megbízhatósági paramétereknek különös jelentősége van. Látni fogjuk, hogy a meghibásodási tényező például ilyen sokat szereplő jellemző, a katalógusokban is általában ezt adják meg (a számjellemzők között fennálló matematikai

összefüggések további elemzésekor látni fogjuk, hogy a szintén katalógusadatként gyakran szereplő MTBF élettartam jellemző éppen ennek a meghibásodási tényezőnek a reciproka).

Ismert függvény	A további függvények számítási módja			
	$R(t)$	$F(t)$	$f(t)$	$\lambda(t)$
$R(t)$	$R(t)$	$1-R(t)$	$-\frac{d}{dt}R(t)$	$-\frac{1}{R(t)}\cdot\frac{d}{dt}R(t)$
$F(t)$	$1-F(t)$	$F(t)$	$\frac{d}{dt}F(t)$	$\frac{1}{1-F(t)}\cdot\frac{d}{dt}F(t)$
$f(t)$	$\int_t^\infty f(\tau)d\tau$ *	$\int_0^t f(\tau)d\tau$	$f(t)$	$\frac{f(t)}{\int_t^\infty f(\tau)d\tau}$
$\lambda(t)$	$e^{-\int_0^t \lambda(\tau)d\tau}$	$1-e^{-\int_0^t \lambda(\tau)d\tau}$	$\lambda(t)\cdot e^{-\int_0^t \lambda(\tau)d\tau}$	$\lambda(t)$

* A τ és t egyaránt időparaméter, a τ a futó koordinátát, t az integrálási határt jelenti

4-1. táblázat: Megbízhatósági számjellemzők közötti összefüggések

4.3. A meghibásodási tényező jellegzetességei

A fentiek szerint a leggyakrabban használt sztochasztikus jellemzők közül egyetlen ismeretében a többi meghatározható, ezért most a leggyakrabban használt számjellemzőt, a meghibásodási tényezőt vizsgáljuk meg részletesebben.

Az elektronikus alkatrészek jelentős részének a meghibásodási tényezője igen jó közelítéssel az **időben állandónak tekinthető.** Ezt a közelítést alkalmazzuk a legtöbbször, mivel

- a valóságot sok esetben igen kis hibával írja le,
- a számítások ebben az esetben végezhetők el a legegyszerűbben, sőt bonyolult rendszerekre a számítás gyakorlatilag irreálisan nehézkes és hosszadalmas lenne időben változó meghibásodási tényezőjű alkatrészek esetén,
- az elektronikus alkatrészek gyártói és forgalmazói nem időfüggvénnyel, hanem egy konstans értékkel specifikálnak szinte minden gyártmányt, így legtöbbször nem is áll rendelkezésünkre más lehetőség.

Először az időben álladó paraméterként kezelt meghibásodási tényezővel foglalkozunk, majd a kivételt képező alkatrészek tárgyalása során, (amelyeknél ez a közelítés nem fogadható el) megnézzük, milyen lehetőségek vannak a valóság pontosabb modellezésére.

A meghibásodási tényező dimenziója **1/idő** jellegű. Ha a tényező az időben állandó, akkor – mint láttuk – megegyezik a jó működési idő **(T_F)** reciprokával. Az idő alapvető mértékegysége az óra lehetne, de ez a megbízhatósági vizsgálatokban túl kis mértékegység, mivel azt jelenti, hogy $T_F = 1$ óra esetén az objektum óránként hibásodik meg. Így az idő szokásos mértékegység az év (8760 óra), vagy még inkább a **10^6,** vagy a **10^9** óra. Ebből a meghibásodási tényezőre adódó mértékegységek:

1/1000 óra = 10^{-3} [1/óra],

$^0/_{00}$ /1000 óra = 10^{-6} [1/óra], vagy a

FIT (**Failure In Time**), ami 10^{-9} [1/óra] értéket jelent.

A $\lambda = 10^{-5}$ [1/óra] esetén a $T_F = 10^5$ óra, azaz kb. 11,5 év. Az ilyen objektum tehát átlagosan tizenegy és fél évig működik hibátlanul. De mivel a meghibásodás az időben bármikor bekövetkezhet, lesz olyan, amelyik korábban és amelyik később működésképtelen. Ebből következik, hogy például egy olyan berendezés, amelyik 11 ilyen terméket tartalmaz, kb. évenként egyszer hibásodik meg átlagosan ezek miatt.

Az alkatrészek meghibásodási tényezőjét a katalógusukban megtalálhatjuk. Nagyságrendi tájékoztatásként szolgáljon az alábbi néhány adat:

- egy integrált áramkör típustól és mérettől függően 1-100 FIT
- egy ellenállás, kondenzátor típustól és mérettől függően 1-10 FIT
- áramköri kötés, csatakozás típustól függően 0,1-1 FIT.

Az időben álladó meghibásodási tényező a **nem öregedő** jelleget (az **örök ifjú**ságot) modellezi. Ez az abszurdnak tűnő modell mégis reális eredményeket ad a gyakorlatban, mivel az örök ifjúság nem az örök életet jeleni, hiszen a várható élettartam ezzel is végesnek adódik ($T_F = 1/\lambda$). Az örök ifjúság csak úgy értendő, hogy egy ideig tartó használat után az objektum ugyanolyan valószínűséggel hibásodik meg egy további használati idő alatt, mint vadonatúj korában ugyanennyi idő alatt. Más szóval nem öregszik. (Ha az örök ifjúság emberre is igaz lenne, akkor egy 80 éves ember ugyan akkora valószínűséggel élné meg a 81-ik évet, mint egy 30 éves a 31-ediket.) Márpedig az elektronikus alkatrészek általában ilyenek, pontosabban szólva, ennek az az oka, hogy amikorra valóban megöregednének, már kimennek a használatból.

Bizonyítás:

Írjuk fel azt a feltételes valószínűséget, hogy exponenciális eloszlás esetén egy objektum túléli a $t_1 + \Delta t$ időtartamot, ha előzőleg már t_1 ideig használtuk, de a t_1 idő végén még üzemképes.

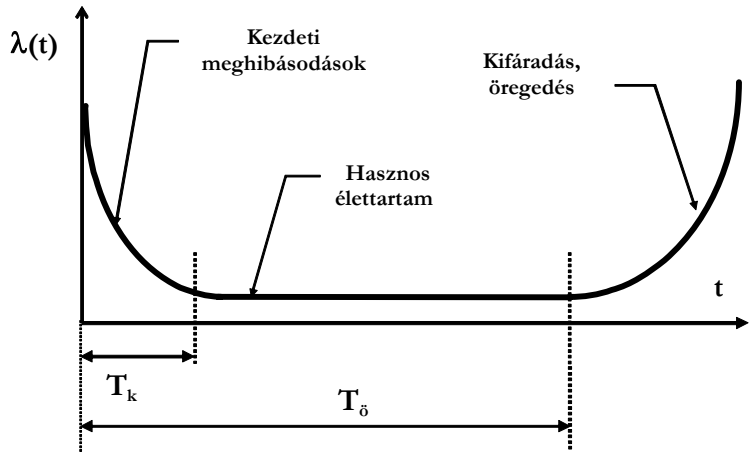
$$R(\Delta t, t_1) = \Pr\left\{T_F > (t_1 + \Delta t) \;\middle|\; T_F > t_1\right\} = \frac{R(t_1 + \Delta t)}{R(t_1)} \qquad (4\text{-}27)$$

A (4-17) képlet felhasználásával:

$$R(\Delta t, t_1) = \frac{\exp\left[-\lambda \cdot (t_1 + \Delta t)\right]}{\exp\left[-\lambda \cdot t_1\right]} = \exp\left[-\lambda \cdot \Delta t\right] \qquad (4\text{-}28)$$

Látható, hogy a feltételes valószínűség nem függ t_1 értékétől, csak Δt-től, tehát közömbös, hogy egy alkalmazást megelőzően meddig használtuk már a terméket, ha a vizsgálatunk kezdetekor még jó. Ez a „nem öregedő" tulajdonság elektronikus alkatrészek nagy részére érvényes.

Amennyiben a meghibásodási tényező **nem állandó** az idő függvényében, akkor az ún. **teknőgörbével (fürdőkádgörbével)** szokták általános érvénnyel jellemezni (a 4-1. ábra szerint).



4-1. ábra: A meghibásodási tényező időbeli alakulása

Ezen a görbén három szakasz különíthető el:

- a **kezdeti meghibásodások** időben csökkenő meghibásodási tényezőjű időszakasza (szokásos elnevezéssel bejáratási időszak), melyre $t \leq T_K$
- az időben stacioner meghibásodási gyakoriságú középső szakasz (a tulajdonképpeni hasznos élettartam), $T_K < t < T_{\ddot{O}}$ és végül
- az elhasználódás, kopás stb. miatti növekvő meghibásodási tényezőjű harmadik (kifáradási, öregedési) szakasz, melyre $t > T_{\ddot{O}}$.

A szakaszok természetesen folytonos átmenettel csatakoznak egymáshoz, az elhatárolás némileg önkényes. Az elektronikus alkatrészek esetében a stacionernél nagyobb gyakoriságú kezdeti meghibásodások tartománya ténylegesen gyakran tapasztalható, az öregedés azonban csak kevés alkatrész esetében jelentkezik a reális alkalmazási (felhasználási) időben. A legtöbbnél λ növekedése akkorra esik, amikor elavul a termék és nem használják már.

A ténylegesen öregedő alkatrészek például olyanok:

- ahol **anyagfogyás** jelentkezik az idő folyamán (katódsugárcső, képcső, elektrolitikus kondenzátor stb.),
- amelyek **mozgó** és ezért **elkopó**, **kifáradó** alkatelemeket tartalmaznak (kapcsolók, jelfogók, billentyűzet, villanymotor stb.),
- ahol **eróziós** folyamatok vannak (áram megszakítók, kapcsolók stb.),
- ahol **anyagvándorlás** jelentkezik (hibrid IC-ben a migráció),
- ahol az érintkező felületeken **oxidáció** vagy más a **vezetőképességet, a mechanikai szilárdságot rontó vegyi folyamat** jöhet létre.

A felsorolást lehetne folytatni, azonban ezeket az alkatrészeket a korszerű elektronikus berendezésekben viszonylag kisebb mennyiségben alkalmazzák, így vagy figyelmen kívül hagyjuk véges élettartamukat, amikor az a használat idejében nem várható, vagy a többi elemtől függetlenül számítjuk a várható élettartamukat és ennek a teljes berendezésre vonatkozó hatását.

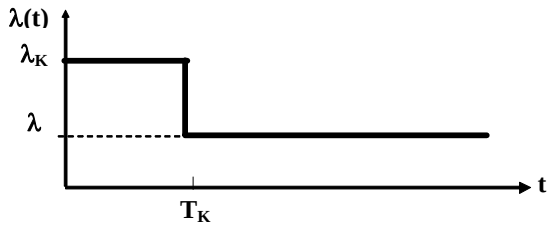
Az alkatrészek zömére viszont a kezdeti meghibásodási szakaszt nem lehet figyelmen kívül hagyni. A gyártástechnológia nem azonnal jelentkező hibái, a gyártásközi ellenőrzés hiányosságai miatt beszerelhetnek a készülékbe olyan alkatrészeket, amelyekben rejtett technológiai, vagy anyaghiba

van (bizonytalan villamos vagy termikus kontaktus, szennyeződés, anyaghiány, vezeték, szigetelés elvékonyodása, oxidáció, ESD miatti károsodás stb.) és ezek hatása nem feltétlenül azonnal jelentkezik, hanem az alkalmazásból adódó (egyébként megengedhető mértékű) igénybevétel során. A bonyolultabb alkatrészek (például mikrokontroller IC, memória IC) gyártásközi és végellenőrzése nem lehet teljes körű. Egyes állapotokat, üzemmódokat nem tudnak megvizsgálni például a vizsgálati idő és költség véges volta miatt. Így azután előfordul, hogy ezekben a hibák csak használat közben jönnek elő, sőt ha az alkalmazásban is csak ritkán előforduló állapotban, memóriacímnél van a hiba, akkor az üzembe helyezés után később okoz üzemképtelenséget.

Mindezek a későbbi stacioner szakaszhoz viszonyítva gyakoribb meghibásodást eredményeznek a kezdeti szakaszban. A jelenség figyelembe vételére a bonyolult képletek helyett a gyártók általában úgy specifikálják a termék megbízhatóságát, hogy a meghibásodási tényező csak egy adott idő után válik állandóvá (veszi fel a specifikációban szereplő névleges értéket), az adott időtartam előtt ($t < T_K$, ahol például $\mathbf{T_K}$ =100-300 óra) a névlegesnél 3-5-ször nagyobb meghibásodási tényezővel kell számolni.

Ezzel tulajdonképpen egy **lépcsős függvényt** adnak meg (4-2. ábra), amit a számítások során figyelembe lehet venni. A meghibásodási tényezőt az (5-17) egyenlet alapján integrálni kell az idő szerint és ez konstans értékekre szakaszosan nagyon könnyen elvégezhető, mivel az integrálás szorzássá egyszerűsödik.

$$R(t) = \exp\left\{-\left[\lambda_K \cdot T_K + \lambda \cdot (t - T_K)\right]\right\} \qquad (4\text{-}29)$$



4-2. ábra: A meghibásodási tényező lépcsős függvénye

4-2. példa:
A lépcsős függvény szerint számított megbízhatóság időfüggvény:

$$R(t) = \exp\left\{-\left[\lambda_K \cdot T_K + \left(t - T_K\right)\right]\right\} = \exp\left\{-\lambda\left[\frac{\lambda_K}{\lambda} \cdot T_K + t - T_K\right]\right\}$$

$$R(t) = \exp\left\{-\lambda\left[t + \left(\frac{\lambda_K - \lambda}{\lambda}\right) \cdot T_K\right]\right\}$$

Tehát a tényleges t időhöz a $\mathbf{T_K}$ idő $\frac{\lambda_K - \lambda}{\lambda} = 2...4$ -szeresét hozzá kell adni.

A lépcsős függvénnyel való számításokat azonban az esetek nagy részében mellőzni lehet és rögtön a stacioner, kisebb meghibásodási tényezővel lehet számolni, mivel az idő jelentős részében még nincs az adott elem a végleges felhasználás körülményei között, hanem:

- a gyártónál van mérés, ellenőrzés stb. miatt
- a felhasználónál (aki beépíti a készülékébe) még szereléssel, méréssel, ellenőrzéssel telik az idő,
- az alkalmazónál (üzemeltetőnél) üzembehelyezés, próba van stb.

A fogyasztói elektronikus készülékek esetében ez az üzemszerű alkalmazás előtti idő kisebb $\mathbf{T_K}$-nál, ezért a terméket **előégetni** kell annak érdekében, hogy a kezdeti meghibásodások szakaszát el lehessen kerülni. Az ilyen előégetést gyakran nagyobb igénybevétellel (magasabb hőmérséklet, nagyobb tápfeszültség) végzik, mint ami a névleges üzemi körülményekből adódik, mivel az időtartamot a költségek és az időveszteség miatt célszerű lerövidíteni és így a hibák korábban előjönnek. A forszírozott stresszel végzett gyorsított vizsgálat persze csak olyan igénybevételt okozhat, amelyik nem okoz maradandó károsodást és csak olyan esetleges hibák előrehozatalát eredményezheti, amelyek normális körülmények között is előfordulnak csak hosszabb idejű használattal.

Az időben változó meghibásodási tényező végül is nem mindig kerülhető el. Ilyen esetekben természetesen nem lehet exponenciális eloszlással számolni. Az elvileg (matematikailag) alkalmazható eloszlások körét a gyakorlati életben valóban szóba jövő esetekre korlátoztuk. Az egyik általáno-

san alkalmazható eloszlás a **Weibull-féle.** Ezzel időben csökkenő és növekvő meghibásodási tényező modellezhető, sőt speciális esetként a konstans meghibásodási tényező is, mivel az exponenciális eloszlás a Weibull eloszlás speciális esete. Az eloszlásfüggvény komplemensét rögtön a céljainknak és jelölésrendszerünknek megfelelő formában írva Weibull eloszlás esetén:

$$R(t) = \exp\left(-\beta \cdot t^{a}\right) = e^{-\beta \cdot t^{a}} \tag{4-30}$$

A Weibull eloszlásra érvényes $\lambda(t)$ időfüggvény pedig a

$$\int \lambda(t) \cdot dt = \beta \cdot t^{a} \tag{4-31}$$

összefüggésből

$$\lambda(t) = a \cdot \beta \cdot t^{a-1} \tag{4-32}$$

Bizonyítás:
A fenti összefüggés egyszerűen adódik, ha az R(t)-re vonatkozó (4-17) és (4-30) összefüggésekben a kitevők egyezését felírjuk:

$$\int \lambda(t) \cdot dt = \beta \cdot t^{\alpha}$$

és az egyenlet mindkét oldalát differenciáljuk.

Ha $\alpha = 1$, akkor a Weibull eloszlás speciális eseteként az exponenciális eloszlás adódik:

$$\lambda(t) = \beta = állandó = \lambda \tag{4-33}$$

Ha $\alpha > 2$, akkor időben növekvő $\lambda(t)$-val az öregedést modellezhetjük, ha $\alpha < 1$, akkor pedig a kezdeti meghibásodási szakaszhoz alkalmas. Az $1 < \alpha < 2$ tartomány egyes redundáns rendszerek modellezésére használható. A Weibull eloszlás esetére vonatkozó várható jó működési idő egy kissé bonyolultabb integrállal számolható célszerűen számítógépet, vagy táblázatot alkalmazva.

Egy további eloszlás, ami a megbízhatóság modellezésére számításba jöhet a **normális (Gauss-féle) eloszlás.** A sűrűségfüggvény ebben az esetben:

$$f(t) = \frac{1}{\sigma \cdot \sqrt{2\pi}} \cdot e^{-\frac{(t-T_F)^2}{2 \cdot \sigma^2}} \tag{4-34}$$

ahol ismert módon

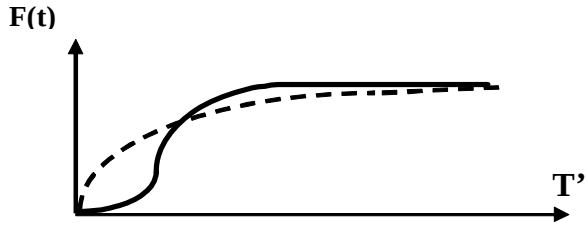
- σ a szórást,
- $\mathbf{T_F}$ a meghibásodási idők várható értékét jelenti (a matematikában a Gauss eloszlás függvényében a $\mathbf{T_F} \equiv m$ jelelölés a szokásos)

Ezt az eloszlást azonban elvileg egyáltalán nem használhatnánk, mivel egy lényeges feltételnek nem felel meg: a $t < 0$ tartomány a megbízhatósági számításokban nincs értelmezve és ez az eloszlás nullánál nagyobb valószínűséget ad ebben a tartományban is és nem teljesíti azt a feltételt, hogy $R(0) = 1$. Így legfeljebb közelítésként használhatjuk akkor, ha a szórás sokkal kisebb mint a várható érték.

Elvileg jobb megoldás a **lognormális** eloszlás. Ezzel azonban azért nem foglalkozunk, mivel elektronikus alkatrészek esetében gyakorlatilag nem állnak rendelkezésre a szükséges paraméterek, de ha esetleg egy alkatrészre mégis rendelkeznénk ilyen adattal, a további számítások részletezése meghaladná a könyv kereteit.

4.4. A javítási tényező jellegzetességei

A következőkben röviden megvizsgáljuk a korábban definiált javítási tényező időfüggését. A (3-16) képlet szerinti javítási tényező csak igen durva közelítéssel tekinthető az időben állandónak. Az üzemképtelen állapotban töltött **T'** időt (3-1. ábra) $\mathbf{T_D}$ várható értékével és annak reciprokával jellemeztük. A **T'** időre vonatkozó eloszlás függvény azonban nem exponenciális, a gyakorlatban a 4-3. ábra folytonos vonalához hasonlóan alakul, mivel **az üzemképtelen állapothoz tartozó és egymást követő folyamatok eloszlásfüggvényeinek egyesítésével jön létre.** Az állandó intenzitást jelentő exponenciális eloszlás (lásd a 3.3.ábrán a szaggatott vonalat) például már rendkívül rövid időn belül is véges valószínűséget szolgáltat a hiba elhárulására, viszont a hiba keletkezése és felismerése közötti időben biztosan nincs javítás. **A folytonos vonal a gyakorlatot jobban jellemezve vízszintes érintővel indul.** A hiba a felismerés után egyes esetekben gyorsan elhárul, például egy csatlakozás érintkezése esetleg egyetlen mozdulattal rendbe hozható. Ez indokolja a folytonos görbe meredekebb emelkedését. Végül az exponenciális eloszlással szemben a javítás még ritkán sem tart végtelen sokáig, tehát az eloszlása sem aszimptotikusan közelíti a végértéket.



4-3. ábra: Az üzemképtelen állapothoz tartozó eloszlás függvény jellege

Egy lehetséges megoldás Weibull eloszlású szakaszokból késleltetésekkel összeállítani a függvényt. Ez számítástechnikailag megoldható, de kissé körülményes. Elfogadható lehet az a közelítés, ha az egyes szakaszokat exponenciális eloszlású darabokból rakjuk össze.

4.5. A megbízhatóság specifikációja, a becslések minősége

A már használatban lévő objektumok megbízhatósági paraméterei a hibastatisztikákból meghatározhatók, ha erre kellő idő rendelkezésre áll. Alkatrészekből **összetett** készülékek, nagyobb rendszerek megbízhatósága a már más berendezésekben korábban alkalmazott elemeik megbízhatósági adatai alapján számolhatók, akár már a tervezési stádiumban is (ezzel a későbbiekben foglakozunk). Elvi számítások helyett célszerűbb, ha van rá lehetőség, a termékekre vonatkozó *vizsgálatok* és *tapasztalatok* alapján becslést adni.

A megbízhatósági paraméterek empirikus meghatározásának, mérésének módszerei alapvetően különböznek a gyártmányok minősítő, minőségellenőrző méréseitől, mivel:

a) vagy csak **utólag,** hosszú idejű alkalmazási tapasztalatból, szerviz statisztikákból nyerhetők, ekkor az eredmények túl későn keletkeznek, nem alkalmasak arra, hogy a termék értékesítése előtt adjanak lehetőséget a specifikálásra.

b) vagy más hasonló termékekre vonatkozó tapasztalatok alapján lehet becslést adni (lásd az 5.2 és a 6. fejezetet),

c) vagy a termékek egy részét forgalomba hozás helyett vizsgálatnak kell alávetni.

A *b)* és *c)* módszerrel nyert adat viszont nem közvetlenül az adott forgalmazott termékre, hanem csak annak típusára lesz jellemző és a forgalomba kerülőkre vonatkozóan becslést ad. (A *c)* esetben a vizsgálatnak alávetettek elhasználódnak). Valós adatok esetében a megbízhatósági jellemzők ilyen módszerrel történő meghatározása csak egy elvi lehetőség, alkalmazásának sajnos nincs sok realitása.

Egy újonnan alkalmazásba vett objektum **várható** jó működési ideje *korábban üzembe állított azonos típusú,* kellő számú objektum kellő időtartamú üzemeltetési adataiból származó **átlagos** jó működési idővel becsülhető, persze ha a kérdéses újabb objektum is azonos környezeti és üzemi körülmények között fog működni. Joggal merül fel a kérdés, mennyire jó a becslés, érvényes-e a típus valamennyi elemére. A kétely a gyakorlatban nagyon is indokolt, hiszen a *c)* változatban a vizsgálatok rendkívül nagy idő és költség igénye miatt viszonylag kevés terméket lehet csak elfogadható ideig tartó vizsgálatnak alávetni. Mint a 4.3 fejezetben a meghibásodási tényezőre vonatkozó adatok és a 6.1 fejezetben a gyorsított vizsgálatokra vonatkozó ismeretek kapcsán belátható, korszerű elektronikus alkatrészek esetében sok ezer alkatrész több ezer óráig tartó vizsgálatára van szükség a gyakorlatban és ekkor is csak egy-két elem hibásodik meg a nagy mennyiségből. Sőt még az is gyakori, hogy az elfogadható vizsgálati idő alatt egyetlen hiba sem keletkezik. Ennek alapján csak azt mondhatjuk, hogy az adott termék jó, de, hogy pontosan mennyire, az nem ismeretes.

A megbízhatóságot azonban már akkor kell specifikálni, a karbantartás, tartalékolás stb. feltételeit akkor kell meghatározni, amikor még *tapasztalat híján statisztikai adatok nem állnak rendelkezésre.* A csak *utólag,* hosszú idejű alkalmazási tapasztalatból, szerviz statisztikákból nyerhető átlag adatok viszont túl későn keletkeznek és ezért nem alkalmasak arra, hogy már a termék értékesítésekor adjanak lehetőséget a specifikálásra. Korszerű elektronikus termékek esetében gyakran még súlyosabb a helyzet, az sem ritka, hogy az ilyen tapasztalati adatok kellő mennyiségben csak akkorra keletkeznének, amikor az adott terméket nem hozzák már kereskedelmi forgalomba, gyakorlatilag alig használják is, mivel elavult. Az ilyenkor nyerhető adatokra az adott termék kapcsán nincs igény, azok legfeljebb **más hasonló újabb termékekre** vonatkozóan hasznosíthatók.

Az aktuális termékek egy részét **forgalomba hozás helyett vizsgálatnak lehet alávetni.** A vizsgáltak persze elhasználódnak és ráadásul a vizsgálatok rendkívül nagy idő igénye miatt későn szolgáltatnak eredményt. Járható út az lehet, hogy **más, hasonló, korábban alkalmazott**

termékekre vonatkozó tapasztalatok felhasználásával **becslés**t adunk. A tapasztalati adatokat az aktuális fizikai-kémiai folyamatok alapján **át kell számítani,** ha a statisztika alapjául szolgáló és a kérdéses objektum között eltérés van az alkalmazásban, a terhelésben, a környezeti feltételekben, illetve ha a teljesítendő funkciókban olyan különbség adódik, ami a hibakritériumok között is eltérést okoz. Az eltéréseket számításba véve az adatokat **extrapolálni** kell.

A megbízhatóság – mint láttuk – többféle paraméterrel és függvénnyel jellemezhető. Bár ezek között összefüggések vannak, mégsem mindegy, hogy egy-egy adott alkalmazáshoz melyik a legmegfelelőbb. A „jó" idő várható értéke (T_F, T_U) például nem igazán alkalmas redundáns rendszerek jellemzésére, ha a termék tényleges felhasználási ideje ennél az időtartamnál sokkal rövidebb, vagy ha rövidebb időközű rendszeres megelőző karbantartás van. Ilyen esetekben sokkal fontosabb a megbízhatóság minimális értékének megadása az adott időintervallumra. Ehhez az r(t) függvényt kell meghatározni. Ha egy folyamatos felügyeletet adó rendszerről van szó, akkor a kiesések időtartama várható értékét a legfontosabb megadni stb.

Jellemzően, de nem kizárólagosan az alábbiak szerint célszerű specifikálni:

λ : alkatrészek esetén (lásd a fejezetben)
$T_Ö$: az *öregedés,* elhasználódás várható ideje (lásd a 4.3 fejezetben)
T_F: elhasználódó, meghibásodás esetén nem javított, *nem javítható* (kiselejtezendő) termékek esetén (lásd a 3.3.4.1 fejezetben),
T_U: meghibásodás esetén **javított,** felújított termékek esetén (lásd a 3.3.4.2 fejezetben),
T_D: folytonos felügyeletet adó rendszerek esetén (lásd a 3.3.4.3 fejezetben),
K: termelő rendszerek esetén (lásd a 3.3.5.1 fejezetben),
DTR: szolgáltatást adó rendszerek esetén (lásd a 3.3.4.3 fejezetben),
R(t): T_{max} ideig működtetett **(**$t \leq T_{max}$), adott küldetésű rendszerek és a *periodikus megelőző karbantartással* ($t=T_{MK}$) üzemeltett redundáns rendszereknél (lásd a 3.3.2.2 fejezetben),
d(t): *eseménykövető felújítással* üzemeltett redundáns rendszereknél (lásd a 4.1 fejezetben).

A termék forgalmazójának versenyképes adatot kell reális időn belül specifikálnia, ezért gyakran egy **határértéket** adnak meg azt szavatolva, hogy a

termékek egy része teljesíti azt, vagy annál is jobb. A meghibásodásig várható működési időre specifikálnak értéket:

$$T_F \geq T_{spec} \tag{4-35}$$

vagy ezzel egyenértékű, ha a meghibásodási tényezőre vonatkozóan:

$$\lambda \leq \lambda_{spec} \tag{4-36}$$

és a specifikált értéket a termékeknek csak megadott hányadára (például 60%, vagy 90%) garantálják. Egyszerűen: ez a hányad a becslés jósága, „hihetősége" a

konfidencia szint = C.

Joggal merül fel a kérdés, mennyire jók a becsléseken alapuló adatok. A kétely a gyakorlatban nagyon is indokolt, hiszen esetleg csak azt állíthatjuk, a termék megbízhatósága a vizsgálat alapján számított vagy annál jobb, de hogy pontosan mennyivel jobb, az nem ismeretes.

A becslés jósága **„megbízhatósága"** azaz konfidencia szintje, a konfidencia intervallum nagyságától függően a mérési eredményekből a matematikai statisztika módszereivel határozhatók meg. A számítások részletezése meghaladja a könyv terjedelmi korlátait, ezért bizonyítás nélkül csak néhány gyakorlati adatot közlünk az alábbiakban a **normális** (Gauss) eloszlás és az **exponenciális eloszlás** esetére.

A $\mathbf{T_F}$ időre (MTTFF) specifikált T_{spec}-re érvényes az alábbi összefüggés, ha a meghibásodási folyamat **normális eloszlás**t mutat. Ez az eloszlás elsősorban a várható élettartamnál lényegesen kisebb szórású, elkopó, elhasználódó alkatrészekre, illetve az elfogyó elemet tartalmazó véges élettartamú termékekre (például kapcsoló, izzólámpa, képcső) elfogadható modell.

$$T_{spec} = \overline{T} - k \cdot \frac{\sigma}{\sqrt{N_0}} \tag{4-37}$$

ahol

- $\mathbf{N_0}$ – a vizsgálatba bevont elemek száma,
- $\overline{T}$ – a vizsgálatokból adódó átlagos jó működési idő,
- $\boldsymbol{\sigma}$ – utóbbi szórása,
- a **k** konstans pedig a **C** konfidencia szinttől függ, például:

C = 60% esetén **k** = 0,25,

C = 90% esetén **k** = 1,28.

Az értékek a normális eloszlás táblázatából származnak (például [19]).

Alkatrészekre vonatkozóan a leggyakoribb esetet, az exponenciális eloszlást feltéve az alábbi összefüggés alkalmazható:

$$\lambda_{spec} = \frac{k}{N_0 \cdot T} \qquad (4\text{-}38)$$

ahol

- **T** – a vizsgálat időtartama,
- $\mathbf{N_0}$ – a vizsgálatba bevont elemek száma,
- **k** – az adott idő alatt meghibásodott elemek számától, **H**-tól és a konfidenciaszinttől (**C**) függő konstans.

Értéke egyszerű esetben a Poisson-eloszlás kvantilisei táblázatából nyerhető. Például H = 0..6 hibával és C = 60, illetve 90%-os konfidencia szinthez az alábbi értékek adódnak:

Legyen	**H =**	0	1	2	3	4	5	6
ha **C**=60%	**k =**	0,92	2,02	3,10	4,17	5,24	6,29	7,34
ha **C**=90%	**k =**	2,30	3,89	5,32	6,69	7,99	9,27	10,53

A $\overline{T}$ átlagidőt és a T mérési időt gyorsított élettartam vizsgálatok alkalmazása esetén a névleges igénybevételnek megfelelő értékre **át kell számítani**, azaz az **a** gyorsítási tényezővel szorozni kell.

$$\overline{T'} = a \cdot \overline{T} \quad \text{illetve} \quad T' = a \cdot T \qquad (4\text{-}39)$$

Más matematikai módszerek és más eloszlások alkalmazása jobb becslést ad a fentieknél. Ez a néhány adat azonban a **gyakorlati esetek jelentős részében elegendő** a számításhoz. Pontosabb és igényesebb statisztikai módszerekre vonatkozóan az irodalomjegyzékre kell hivatkoznunk [8], [17].

4-3. példa:

Egy konstans meghibásodási tényezőjű alkatrészből N = 1000 darabot T = 500 órás a = 40-szeres gyorsítással vizsgálatnak vetnek alá. Ez idő alatt H = 1 db hibásodik meg. A meghibásodási tényezőre határértéket kívánnak specifikálni C = 60% konfidenciával.

$$\lambda_{spec} = \frac{k}{N \cdot T \cdot a} = \frac{2,02}{1000 \cdot 500 \cdot 40} \approx 10^{-7} \left[\frac{1}{ó}\right]$$

Az alkatrész adatok tehát meglehetősen bizonytalanok, bár a különböző gyártmányok összehasonlítására azért alkalmasak, ha a specifikációs-becsléses módszerek azonosak. Ez utóbbit a gyártó cégek kiadványaikban leírják. De az ilyen **alkatrész adatokból** számított megbízhatósági **rendszerparaméterek**et az üzemeltetés tapasztalataival összevetve nyilvánvalóan nem ritka, hogy számottevő eltérés adódik. Az eltérések természetesen szinte kizárólag az előrejelzések túlzott pesszimizmusára utalnak: a tapasztalt jó működési idő az alkatrészek adatai alapján számított eredőhöz viszonyítva esetleg kétszer-háromszor nagyobb lehet.

Az ellentmondás okai:

1. **Hibásak az alkalmazott alkatrészadatok:**
   A vizsgálatokból származó specifikált alkatrészadatok sokkal jobbak a tapasztaltnál, mivel az előző pontban ismertetett módon *egyoldalas konfidencia intervallumra* és csak 60%-os konfidenciaszinttel értelmezték. Nem ritka az sem, hogy egyes alkatrészek megengedett *toleranciája kisebb a szükségesnél* és ezzel rejtett és csak igen körülményesen számításba vehető redundancia van a rendszerben drift jellegű meghibásodási folyamat esetén, ilyen az alkatrész toleranciájának kisebb túllépése.
2. **Hibás az üzemeltetés körülményeinek számításba vétele:**
   Az üzemeltetéskor a stresszt (terhelést) a legrosszabb esetre számították, de annál kisebb, vagy az igénybevétel nem folytonos és a szakaszos terhelésből adódó **derating**-et nem vették figyelembe.
3. **Hibás a rendszer struktúrájának modellezése:**
   A struktúra modellezésekor elhanyagoltak egyes rejtett redundanciákat, például az alkatrésznek egyes hibáit, amelyek nem katasztrofálisak és nem okoznak a rendszerben üzemképtelenséget. Gyakran számításba vesznek olyan elemeket is, amelyek az adott alkalmazásban teljesen feleslegesek, vagy csak elhanyagolható valószínűséggel válhatnak szükségessé.

Mindezek a hibák a modellezés és a számítások finomításával csökkenthetők, de az így adódó eltéréseket gyakran egyszerűen biztonsági tartaléknak tekintik. Nemzetközileg elterjedt az általános jelleggel **egyáltalán nem igazolható** úgynevezett egyharmados törvény. Eszerint a tényleges alkalmazások során a rendszerre vonatkozó tapasztalati értékek a becsléssel specifikált meghibásodási tényezők alapján számított eredőnek harmada körül adódnak.

5. A megbízhatóság modellezése

5.1. Modellekről általában

A minőség szempontjából vizsgált objektum (nemcsak a nagyberendezések és rendszerek, de egy egyszerű alkatrész is) a valóságban túlzottan bonyolult ahhoz, hogy teljességében vizsgáljuk, hogy valamennyi kisebb hatású befolyásoló tényezőt figyelembe vegyünk. Egyes adatok elhanyagolhatóan csekély hatása a mérnöki munkában igen gyakran egyszerűsítéseket tesz lehetővé, illetve szükségessé. Ezért egy **modellt** hozunk létre, amely egyszerűbben kezelhető és azt analizáljuk. Ezt kell tennünk a biztonsági és megbízhatósági analíziskor is.

A modellnek tehát

- a valóságnál egyszerűbbnek, áttekinthetőbbnek kell lennie
- a feltett kérdésekre közel azonos választ kell adnia, mint a valóság
- csak a lényegtelen dolgokat hagyhatja figyelmen kívül
- lehetővé kell tennie matematikai módszerek alkalmazását
- módot kell adnia arra, hogy szükség esetén kiegészíthessük, finomíthassuk.

A vizsgálat tárgyát képező rendszert, objektumot szokás referensnek nevezni, ennek reprezentációja, megjelenítése során valósítjuk meg a rendszer céltudatosan leegyszerűsített képét. Ez megőrzi a referens kiválasztott jellemzőit, figyelmen kívül hagyva azon sajátosságait, amelyek az adott szempontból nem fontosak, ezért elhanyagolhatók. A rendszer legegyszerűbb leírása az azt alkotó elemek és a köztük fennálló kapcsolatok megadásával (szóban, verbálisan, esetleg bizonyos matematikai apparátussal, szemiformális módon, vagy teljesen kötött formában, ún. formális módszer segítségével) történhet. A modell ezek után úgy definiálható, mint a referens megjelenítése valamely véges és formális (kötött alakú) rendszer segítségével. A rendszer reprezentációját mindig a célszerűség szempontjainak megfelelően kell létrehozni, a specifikus referens alapján. A reprezentáció kialakítása során fontos az egyszerűsítés mértékének és a kiválasztott jellemzőknek a meghatározása. A modell általában kötött alakú rendszer, matematikai vagy logikai struktúra, amely a referens tulajdonságait, azok választott jellemzőit és a köztük fennálló kapcsolatokat tükrözi. Az ehhez szükséges elemek adják meg a modell szintaxisát (egyenletrendszerek, gráfok, műszaki rajzok, kapcsolási rajzok, számítógépes programok stb.).

Ezek teszik lehetővé a rendszertulajdonságok, a modell szemantikájának meghatározását. Ezzel a rendszer vizsgálata mintegy formális következtetési rendszer segítségével végezhető, amivel a módszer megbízhatósága jelentősen növelhető. A rendszer életciklusa során alkalmazható verbális, fél-formális és formális módszerekről a későbbiekben még szólunk.

Az alkatrészek igénybevételét, a funkcionális terhelések hatását a megbízhatóságra a **stressz modellel,** a bonyolultabb rendszereket különböző **struktúra modell**ekkel vizsgáljuk. Ilyen például a **megbízhatósági blokkséma,** a **hibafa elemzés** (FTA), illetve az ún. **hibahatás elemzés** (FMEA). Ezek alapvető alkalmazási feltétele, hogy a rendszernek csupán két állapota legyen, a vizsgálathoz elég legyen a hibás és hibátlan állapot figyelembevétele, s a rendszer monoton jellegű legyen. (E feltételek pontos jelentését a 7.3.1 fejezetben tárgyaljuk). E modelleket összefoglaló elnevezéssel Boole-féle modelleknek nevezzük.

A gyakorlatban előforduló rendszerek esetén ez gyakran nem elegendő, a rendszer lehetséges állapotait és az eseményeket (például meghibásodás, javítás) egy **állapottér modellel** írhatjuk le olymódon, hogy az analízisük elvégezhető legyen. Ezek az ún. Markov-típusú modellek. Ezekről később, a rendszerek megbízhatóságával foglalkozó fejezetben foglalkozunk részletesen.

A vizsgálat jellegétől függően alkalmazható az ún. **fekete-doboz modell,** amely szigorúan az input/output jellegű vizsgálatokat teszi lehetővé. A fekete doboz modell más leírási módoktól függetlenül csak azt írja le, hogy a rendszer bizonyos bemeneti jellemzőihez milyen kimeneti jellemzők tartoznak. Más esetekben végig kell követni, hogy milyen kisebb egységek milyen összekapcsolódásaival épül fel a rendszer. Ezek az ún. **strukturális modellek** hierarchikus szerkezetűek: a nagyobb egységek kisebbekből épülnek fel egymás felett több szinten. A bonyolult hardver objektumokat **funkcionálisan** vizsgálva egy olyan blokksémát látunk, ahol az egyes **dobozok** adott bemeneti gerjesztésre adnak adott választ. Ugyanezt a hardver objektumot **konstrukciósan** elemezve az előzőt nem minden ponton fedő konstrukciós struktúrát látunk, ahol alkatrészekből modulok, áramköri kártyák, műszerfiókok stb. épülnek fel. A **megbízhatósági modellt** úgy kell létrehozni, hogy mindkét előző struktúrát alapul vesszük. Tudniillik arra a kérdésre, hogy egy adott hibajelenség esetén milyen funkciók esnek ki, az egyik, hogy melyik alkatrészt vagy kártyát kell kicserélni, javítani, a másik struktúra alapján adhatunk választ. Már pedig a biztonsági

és megbízhatósági analízis során, sőt az objektum alkalmazásakor is pontosan ezeket a kérdéseket kell megválaszolni.

Amennyiben a funkcionális és a konstrukciós struktúra azonos (minden egyes funkcióhoz jól elkülönülő modulok, alkatrészek tartoznak), akkor a megbízhatósági modellt nem kell külön létrehozni, mivel az azonos az előző két egymással átfedésben lévő struktúrával. Ha viszont a funkcionális és a konstrukciós struktúra csak helyenként fedi egymást (és ez a sokkal gyakoribb), akkor **a megbízhatósági struktúra egy harmadik modell,** amit úgy kell létrehozni, hogy mindkét struktúrának megfeleljen. Ez a gyakorlatban egyszerűen megalkotható: az eljárás az, hogy amennyiben a konstrukciós egység több külön kezelendő funkcióhoz tartozó részegységeket tartalmaz, akkor ezeket a funkcionális részegységeket kell a megbízhatósági struktúra elemeinek választani. Ha pedig egy adott funkciót több konstrukciós modul lát el, akkor ezek a kisebb konstrukciós egységek lesznek a megbízhatósági struktúra építőkövei.

Másképpen fogalmazva: a kétféle alapstruktúrából úgy kell a megbízhatósági modellt készíteni, hogy ebben mindig a kevesebb elemet tartalmazó egység alkosson építőkövet.

5-1. példa:

Ha egy nyomtatott áramköri kártyán több elválasztható funkcióhoz tartozó elemek vannak, akkor a megbízhatósági modellben nem az egész kártya, hanem az egyes funkciókhoz tartozó alkatrészek vagy részegységek alkotnak építőkövet, ha viszont egy adott funkcióhoz tartozó hardver több kártyán helyezkedik el, akkor az egyes kártyák alkotják a megbízhatósági struktúra elemeit.

A gyakorlatban egy hiba esetén kártyát, alkatrészt kell cserélni, ezekből kell tartalékkészlet stb., mindez nem rendelhető közvetlenül mindig a hibás funkcióhoz. A biztonság viszont adott funkciók rendelkezésre állásától függ.

A minőségbiztosítás területén alkalmazott modellek az ún. leíró, előíró és prediktív modellek. A **leíró modell**el a rendszert jellemző referens választott jellemzőit, az **előíró modell**el a rendszer által teljesítendő követelményeket kell leírni, utóbbival lehetővé téve a rendszer tesztelését. A **prediktív modell** segítségével a rendszer jövőbeli viselkedése elemezhető.

A **termék-folyamat modell**ezés a rendszertervezés, a szervezeti stratégiák kialakítása és a minőségirányítás problémáinak megoldását teszik

lehetővé. A termék és a folyamat a minőségirányítás kulcsfogalmai. A termék fekete dobozként modellezett, időponthoz kötött rendszer, az őt előállító folyamattól függetlenül meghatározható, mint tulajdonságmértékek és ezek kapcsolatainak halmaza. A folyamat szintén fekete dobozként modellezett, időponthoz kötött rendszer, amely egy bemenő terméket kimenő termékké alakít. Itt is tulajdonságmértékekkel és közöttük lévő relációkkal írható le a modell. A tulajdonság mértékek lehetnek a

- folyamat bemenő termékeinek tartománya,
- e bemenő termékek tulajdonság mértékein végrehajtott műveletek,
- folyamat időtartama,
- folyamat foglaltsági állapota.

Ilyen módon a folyamat a bemenő és kimenő termékek átviteli függvényének tekinthető. Aszerint, hogy a bemenő és kimenő termékek tulajdonság változói és azok értékei milyen módon alakulnak a folyamat során, a következő folyamat típusokat lehet megkülönböztetni:

- **tárolási folyamat** (a tulajdonság változók és azok mértékei változatlanok maradnak),
- **részleges tárolási folyamat** (a tulajdonság változók száma legalább eggyel csökken),
- **értékadó folyamat** (a folyamat a bemenő termék minden tulajdonság változóját megőrzi és azok mértékei nem feltétlenül maradnak változatlanok),
- **részleges értékadó folyamat** (a folyamat a bemenő termék minden tulajdonság változóját megőrzi és legalább egy új változót létrehoz, a tulajdonság változók mértékei ennek megfelelően változ(hat)nak),
- **generatív folyamat**ok (mindazon folyamatok gyűjtő fogalma, amelyeknél a kimenő termékben szereplő tulajdonság változók és azok mértékei eltérnek a bemenő termékétől).

5.2. Megbízhatósággal kapcsolatos analízis és szintézis feladat

A **megbízhatóság analízisére** több módszer ismeretes. Ezek közül a terjedelmi korlátokat szem előtt tartva csak néhányat ismertetünk, de azért figyelembe véve, hogy

- a gyakorlatban előforduló valamennyi lényeges kérdésre választ adjanak,
- csak a lehető legegyszerűbb matematikai apparátust igényeljék.

A **megbízhatóság szintézise,** azaz a biztonsági és megbízhatósági követelmények teljesítésére irányuló tervezés, közvetlenül nem végezhető el, csak iteratív analízissel oldható meg. Egyszerűen fogalmazva: a tervezett megoldás analízisét elvégezve, a szükséges módosításokat követően újabb megbízhatósági analízis szükséges, majd újabb módosítás, újabb analízis stb. A szintézis tehát módosítások és elemzések sorozatával valósul meg.

Mint a 4.5 fejezetben láttuk, egy adott objektum megbízhatósága az alkalmazásból származó tapasztalati adatok alapján statisztikai módszerekkel is elemezhető. A tapasztalati adatokat az aktuális fizikai-kémiai folyamatok alapján **át kell számítani,** ha a statisztika alapjául szolgáló és a kérdéses objektum között eltérés van az alkalmazásban, terhelésben, a környezeti feltételekben, illetve ha a teljesítendő funkciókban olyan különbség adódik, ami a hibakritériumok között is eltérést okoz.

A korszerű elektronikus termékek esetében gyakran még súlyosabb a helyzet, mivel a megbízhatóságot akkor kell specifikálni, a karbantartás, tartalékolás stb. feltételeit akkor kell meghatározni, amikor még tapasztalat híján statisztikai adatok nem állnak rendelkezésre. Sőt az sem ritka, hogy az ilyen tapasztalati adatok kellő mennyiségben csak akkorra keletkeznének, amikor az adott terméket már gyakorlatilag alig használják és egyáltalán nem is hozzák már kereskedelmi forgalomba, mivel elavult. Az ilyenkor nyerhető adatokra az adott termék kapcsán nincs igény, legfeljebb más hasonló újabb termékekre vonatkozóan hasznosíthatók.

Ezért az esetek döntő többségében a megbízhatósági becsléseket más, hasonló objektumokra vonatkozó korábban keletkezett tapasztalatokat felhasználva, az eltéréseket számításba véve **extrapolálni kell.** Érvényes ez akár egy újabb számítógéptípusra, vagy egy a korábbi technológiával gyártott újabb típusú integrált áramkörre.

A **megbízhatósági analízis** ilyen esetben az alábbiakat jelenti:

- Az objektum funkcióinak pontosítása.
- A minőségi állapotok (paraméterek, tűrési tartományok, határértékek), hibakritériumok rögzítése.
- A funkcionális és a konstrukciós struktúra alapján a megbízhatósági modell megalkotása.

- A modellre érvényes megbízhatósági összefüggések meghatározása.
- Az objektumot alkotó elemek, alkatrészek megbízhatósági adatainak és stressz-függvényeinek meghatározása (tapasztalati és katalógus adatok feldolgozásával, szakirodalom felhasználásával).
- A környezeti és terhelésbeli paraméterek aktuális értékeinek meghatározása (mérések, áramköri számítások, alkalmazási feltételek, specifikáció, használati utasítás).
- Az objektumot alkotó elemek aktuális megbízhatósági paraméterének kiszámítása (stressz függvények, táblázatok, számítógépes módszerek).

Az objektum megbízhatóságának kiszámítása.

- a funkcionális és a konstrukciós struktúra alapján a megbízhatósági modellt megalkotva a modellre érvényes megbízhatósági összefüggések segítségével, vagy
- a rendszer lehetséges állapotainak a hibakritériumok szerinti rendezését követően az állapotok közötti átmenetekhez tartozó paraméterek meghatározásával az egyes állapotok valószínűségének számítása útján analitikus vagy szimulációs eljárással.

Az elemzés (analízis) irányát tekintve a rendszer lehetséges minőségi állapotai alapján, az egyes állapotok közötti átmenetekre (meghibásodások, javítások) vonatkozó ok-okozati és valószínűségi összefüggések felhasználásával két eljárás létezik:
A vizsgálat

- a rendszer lehetséges állapotaiból kiindulva az adott állapotban bekövetkezhető események szerint „felülről lefelé”, vagy
- a lehetséges elem hibákból kiindulva azoknak a rendszerre gyakorolt hatásai szerint „alulról felfelé” szerveződhet.

Előbbi esetben az angolszász terminológiával szokás **top-down,** utóbbiban **bottom-up** eljárásról beszélni. A korábban említett modelleket tekintve a hibafa elemzés tekinthető példának a top-down, a hibahatás elemzés a bottom-up eljárásra. A későbbiekben még lesz szó ezekről a módszerekről.

6. Alkatrészek vizsgálata a stressz modell alapján

6.1. A stressz modellről általában

Valamennyi objektum a használat következtében funkcionális terhelésnek van kitéve és a környezet (klíma, szállítás stb.) az üzemi viszonyokkal összefüggésben (de még üzemen kívül is) igénybevételt okoz. Ezek a funkcionális és környezeti igénybevételek a stresszorok. Minden stresszor egy adott határérték felett azonnali teljes mértékű tönkre menetelt: **katasztrofális meghibásodást** eredményez. Például egy kondenzátor átüt és zárlatos lesz a ráadott feszültség egy adott értékének túllépésekor, a félvezető eszköz egy adott hőmérséklet felett végérvényesen meghibásodik.

A stresszorok azonban a kritikus határérték alatt is befolyásolják az objektum meghibásodási folyamatait: a stressz növekedése a meghibásodási tényező növekedését okozza. A stresszorok hatását a meghibásodási tényezőre döntően tapasztalati, de fizikai és kémiai folyamatok elméletére alapozott, az adott elemre érvényes modellel számítják.

A stressz modell két alapvető gyakorlati cél szolgál:

- A tervező, felhasználó, üzemeltető ennek segítségével határozhatja meg, hogy az adott alkalmazói környezet körülményei között milyen aktuális meghibásodási tényezőre számíthat.
- A termék gyártója a névleges meghibásodási tényező specifikálásához szükséges vizsgálati idő lerövidítésére gyorsított eljárásokat használ.

Ez utóbbinak rendkívül nagy a gyakorlati értéke, mivel a meghibásodási tényező meghatározásához igen sok elem (alkatrész) igen hosszú ideig tartó üzemeltetési tapasztalataira lenne szükség. Ha például valós üzemi körülmények között egy 1 FIT-es alkatrészből 100.000 darabot próbapadon üzemeltnek, több ezer órás vizsgálati idő után lehet csak megfelelő adatot (elfogadható hibájú becslést) képezni. Ez ilyen formában megengedhetetlenül sok időveszteséget és költséget okozna, hiszen specifikált megbízhatósági adat nélkül a termék nem piacképes, viszont a forgalomba hozatalt gazdasági okok miatt nem lehet évekig késleltetni.

Végül is gyorsított vizsgálati eljárásokat alkalmaznak, ahol a névlegesnél nagyobb stressz következtében elfogadható időn belül keletkezik megfelelő konfidenciájú statisztikai eredmény. Ahhoz persze ismerni kell a

stresszorok hatását, azaz az aktuális **gyorsítási tényező**t, hogy végül is a névleges viszonyokra érvényes adatot lehessen specifikálni a vizsgálat során kapott eredményeket extrapolálva.

A *gyorsított élettartam vizsgálat*ban csak olyan fajtájú és mértékű forszírozást (stressz növelést) szabad alkalmazni, amelyre érvényes, hogy

- ezáltal kizárólag olyan hibák keletkezhetnek, amelyek normális üzem esetén is előfordulnak, csak akkor sokkal ritkábban,
- ismert a gyorsítási függvény.

A forszírozás feltételeinek és a gyorsítási függvénynek a meghatározására a lépcsőzetes igénybevétel növelés módszerét **(step stress)** alkalmazzák. Ennek a lényege az, hogy a stresszorokat lépésenként növelve megfigyelik, milyen fizikai kémiai folyamatok okozzák a meghibásodásokat. Amennyiben új, a normális üzemben már nem jelentkező hatás adódott, a forszírozás a vizsgálatban nem érheti el az adott stresszor értéket.

Az aktuális és a névleges meghibásodási tényező viszonyát a névleges és az üzemi stressz értékének ismeretében az adott alkatrészre vonatkozó modell alapján egy rendszerint többváltozós függvényből számított, gyorsítási tényezővel határozzuk meg:

$$\frac{\lambda_{ü}}{\lambda_n} = \alpha(\underline{S}) \qquad (6\text{-}1)$$

A képletben alkalmazott jelölések értelmezése a következő:

- $\lambda ü$ az üzemi meghibásodási tényező
- λn a névleges meghibásodási tényező
- $\alpha( )$ a gyorsítást az adott alkatrészre megadó függvény
- $\underline{S}$ a relatív stresszorokból álló vektor

A stresszorokat a névlegesre viszonyított relatív aktuális üzemi értékükkel kell a képletbe behelyettesíteni. Például:

a feszültség stresszor: $S_U = U_ü / U_n$
a teljesítmény stresszor: $S_P = P_ü / P_n$
a hőmérséklet stresszor: $S_\vartheta = \Delta\vartheta = \vartheta_ü - \vartheta_n$
ahol az **ü** az üzemi, **n** a névleges érték indexe.

Így például, ha a stresszor-vektort a fenti három stresszor alkotja:

$$\underline{S} = [S_U, S_P, S_\vartheta] \qquad (6\text{-}2)$$

Az üzemi hőmérséklet implicit formában több stresszorban is előfordul, például a $\mathbf{P_n}$ névleges teljesítmény nem mindig egy specifikált állandó érték, hanem önmagában is a környezeti hőmérséklettől függő változó.

Az $\alpha = \lambda_ü/\lambda_n$ viszonyt azért nevezik **gyorsítási tényező**nek, mert ez adja meg, mennyivel gyorsabban hibásodik meg az objektum stressz következtében, ha α nagyobb mint 1. Például $\lambda_ü/\lambda_n = 2$ azt jelenti, hogy a jó működés várható időtartama a felére csökken. Az üzemeltetés során azonban inkább **lassításról** kell beszélni, mivel a nagyobb megbízhatóság érdekében legtöbbször aláterhelést **(derating)** alkalmaznak, amikor α kisebb 1-nél

A gyorsítási tényező függvénye gyakran egy többváltozós bonyolult függvény. Közelítő jelleggel – főleg ha nem számítógépet alkalmazva határozzák meg a meghibásodási tényezőt – egy egyszerűbb formát is használnak: ilyenkor az egyes stresszorok hatását külön külön számolva az adódó gyorsítási tényezőket szorozzák:

$$\alpha = \prod \alpha_i(S_i) \qquad (6\text{-}3)$$

ahol a fenti példa esetén $\mathbf{S_i}$ helyére sorra $\mathbf{S_U}$, $\mathbf{S_P}$, és $\mathbf{S\vartheta}$ a megfelelő gyorsítási függvény kerül.

$$\alpha = \alpha_U(S_U)\cdot\alpha_P(S_P)\cdot\alpha_\upsilon(S_\upsilon) \qquad (6\text{-}4)$$

A későbbiekben megadunk egy-két $\boldsymbol{\alpha_i}$ gyorsítási függvényt.

6.2. Alkatrészek meghibásodási ráta-értékét befolyásoló tényezők (stresszorok)

A stresszorok két csoportba sorolhatók:

a) **Funkcionális terhelés:** a vizsgált rendszer működéséből adódó igénybevétel
Például: ellenállásnál a disszipált teljesítmény, kondenzátornál a feszültség és az áram, tranzisztornál a disszipált teljesítmény, az áram és a feszültség, kapcsoló elemnél a maximális megszakítandó áram és feszültség.

b) **Környezeti igénybevétel:**
Ezek közül a legdöntőbb rendszerint a hőmérséklet, de ezen túl számos stresszor befolyásolja a megbízhatóságot. Ilyenek: a fizikai hatá-

sok (gyorsulás, rázás, légnyomásváltozás, UV, röntgen, gamma stb. sugárzások), a vegyi hatások (a levegő nedvesség-, só-, kéntartalma stb.).

Az USA alapvetően katonai célra készített, de igen széles körben alkalmazott megbízhatósági kézikönyve (MIL HDBK 217) kb. két tucat környezeti kategóriát különböztet meg és adja meg az összefüggéseket a névleges és az üzemi meghibásodási tényező között bonyolult képletekkel, nagy táblázatokkal. A különböző alkalmazási esetekre egy sor figyelembe veendő tényezőt szab meg a szabvány, különböző π faktorok formájában. Ilyen tényezőket határoz meg például a következők szerint:

- π_V – feszültségterhelés figyelembevételére
- π_S – áramterhelés figyelembevételére
- π_{S2} – átütési feszültség figyelembevételére
- π_F – alkalmazott technológia figyelembevételére
- π_C – komplexitás figyelembevételére
- π_V – érintkező-elrendezés figyelembevételére
- π_{SR} – váltakozó áramú ellenállás figyelembevételére
- π_E – környezeti tényező figyelembevételére
- π_Q – minőségi fokozat figyelembevételére
- π_T – termikus igénybevétel figyelembevételére stb.
- π_L – az alkalmazott technológia konszolidációját veszi figyelembe

A kézkönyvben szereplő összefüggések bonyolultságának illusztrálására következzen két példa:

A **félvezetőkre vonatkozóan** a fenti lehetséges tényezők közül az alábbiak figyelembevételét javasolja a szabvány:

$$\lambda = \lambda_b \cdot \pi_E \cdot \pi_A \cdot \pi_Q \cdot \pi_R \cdot \pi_S \cdot \pi_C$$

ahol

- λ_b a meghibásodási tényezőnek egy a környezeti hőmérséklettől és egyéb tényezőktől függő alapértéke és a
- π faktorok is különböző környezeti kategóriák alapján bonyolultan meghatározható értékeket jelentenek.

Néhány környezeti kategória a szabványból: földi rögzített telepítésű, hordozható, gépjárművön alkalmazott, sós ködnek kitett, rakétán, ágyúból kilőtt stb.

Az ellenállásokra vonatkozóan a szabvány a következő előzőhöz hasonló felépítésű képletet javasolja:

$$\lambda = \lambda_b \cdot \pi_E \cdot \pi_Q \cdot \pi_R$$

Következzen néhány tényezőre vonatkozó érték:

- a π_Q a gyártás minőségétől függ a következők szerint:
  - π_Q <1 speciális gyártmány, külön megállapodások szerint készítik
  - π_Q =1 professzionális termék
  - π_Q >1 a szórakoztató elektronika elemei
  - π_Q = 10...20 minősítés nélküli gyártók
- a π_L az alkalmazott technológia konszolidációjától függ a következők szerint
  - π_L = 1 valamennyi stabil technológiára
  - π_L = 1..10 újabb technológiákkal készült termékre.

A további tényezők részletezésétől eltekintünk, hivatkozva a nevezett kézikönyvre.

A fenti számításokhoz már több számítógépes programot készítettek és hoztak forgalomba világszerte. A gyorsításra vonatkozó képletek, táblázatok rendkívül költséges és időigényes vizsgálatok eredményeként keletkeztek. Elméleti kutatásokon, fizikai kémiai folyamatok sebességére vonatkozó összefüggéseken, sok alkalmazói szerviz statisztika feldolgozásán alapulnak. Ennek ellenére nem egy esetben vitathatóak a gyakorlatban használatos összefüggések. A szakirodalomban kritikák, módosító javaslatok jelennek meg gyakran. Az említett USA katonai kézikönyvnek is több frissített, kiegészített, javított változata ismeretes. Ezen a kézikönyvön kívül használatos más számítási eljárás rendszer (francia, japán), de egyik sem tekinthető tökéletesnek. A legelterjedtebben nemzetközileg az amerikai adattárat használják nemcsak a katonai, de a civil szférában is. Egyes nagy világcégek kötelező jelleggel előírják az alkalmazását a szállítóik részére és saját felhasználásra. A MIL kézikönyv elfogadását tekintsük megállapodásnak, ami révén az esetleges tévedéseket, hibákat kölcsönösen tudomásul veszik és elfogadják az alkalmazó felek.

Az elvi összefüggések bemutatására két gyorsítási függvényt mutatunk be.

A kondenzátorok meghibásodási tényezőjének feszültségfüggése

A feszültségre vonatkozó összefüggés:

$$\alpha_U = (S_U)^n \tag{6-5}$$

ahol **n** a kondenzátor típusától függő konstans.

A fenti összefüggés tapasztalati jellegű és az $\mathbf{S_u} = \mathbf{U_ü}/\mathbf{U_n}$ adott szűkebb értéktartományára használható. (Igen kis és igen nagy stressz esetén már nem érvényes.)

Kondenzátor esetében nemcsak a rákapcsolt feszültség stresszor, a hőmérséklet is erősen befolyásolja a meghibásodási tényezőt. Továbbá egy tápegység puffer-kondenzátora esetében például igen fontos az a maximális áram érték is, ami a bekapcsoláskor a folytonos üzemi értéket erősen meghaladhatja. Végül is a kondenzátorra a feszültség, a hőmérséklet, a maximális áramot korlátozó ellenállás értéke szolgáltat egymással is függésben lévő stresszorokat.

A három stresszorból a következő alakú bonyolult képlet vagy diagramsorozat alkalmazásával kaphatjuk meg az eredményt.

$$\alpha_C = \alpha(S_U, S_R, S_\vartheta) \tag{6-6}$$

Hőmérsékletfüggés

Az alkatrészek meghibásodási tényezőjének hőmérsékletfüggését leggyakrabban az **Arrhenius-törvény** alapján számítják (August Arrhenius – Nobel-dijas svéd vegyész, fizikus, 1859–1927). Ez a fizikai és kémiai folyamatok sebességére vonatkozó ismert és bizonyítható összefüggés, ami általános jelleggel érvényes és elméleti alapon határozhatók meg a képletben szereplő paraméterek.

Egy elektronikus alkatrész esetében a meghibásodást előidéző folyamatok sokrétűsége miatt és mivel ezek közül a folyamatok közül egy-egy alkatrész esetében nem valamennyi, csak egyesek hatékonyak, tekintsük empirikus összefüggésnek az Arrhenius törvényt, ahol a meghibásodási folyamatokra vonatkozó paraméter, az **aktivációs energia** tapasztalatokon és nem elméleti alapokon nyugszik.

$$\frac{\lambda_{ü}}{\lambda_n} = \exp\left[\left(\frac{E_A}{k \cdot \Theta_n}\right) - \left(\frac{E_A}{k \cdot \Theta_{ü}}\right)\right] \tag{6-7}$$

ahol

- $\mathbf{E_A}$ - a látszólagos aktivációs energia [eV]
- $\mathbf{k}$ - a Boltzmannn állandó 8,6·10-5 [eV/K]
- $\mathbf{\Theta_n}$ - a névleges hőmérséklet [K]
- $\mathbf{\Theta_ü}$ - az aktuális üzemi hőmérséklet [K]

$\mathbf{E_A}$ előforduló értéktartománya esetünkben 0,1...1 eV. A számítások egyszerűsítésére alkalmazhatjuk az

1 eV/k = 1,16 104 K

értéket, így

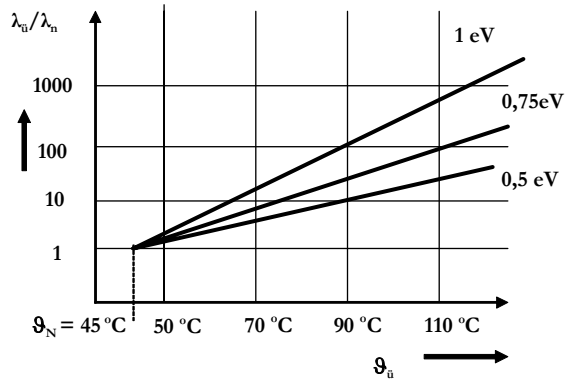
$$\frac{\lambda_{ü}}{\lambda_n} = \exp\left\{1{,}16\cdot 10^4 \cdot E_A\left[\left(\frac{1}{\Theta_n}\right)-\left(\frac{1}{\Theta_{ü}}\right)\right]\right\} \qquad (6\text{-}8)$$

Az aktivációs energiát itt is eV-ban, a hőmérsékletet K-ben kell helyettesíteni. Megjegyezzük, hogy az Arrhenius törvény képletét diagram formájában a félvezető elemek gyártmányismertető katalógusai is rendszerint tartalmazzák.

Az $\mathbf{E_A}$ látszólagos aktivációs energia értékére vonatkozó adatokat a 6-1. táblázat mutatja.

TTL SSI	0,2 eV
PROM	0,4 eV
MOS	0,5 eV
LED	0,6 eV
Lineáris IC	0,7 eV
Planáris elem	1,0 eV
oxidáció	0,3-0,6 eV
migráció	0,5-1,6 eV

6-1. táblázat: Látszólagos aktivációs energia értékei

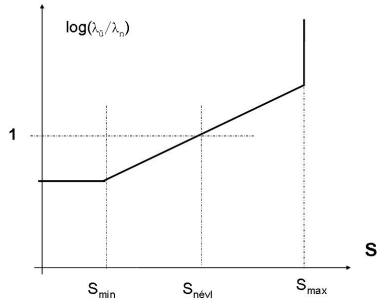


6-1. ábra: Gyorsítási tényező az Arrhenius törvény szerint

A gyorsítási tényező gyakorlatban alkalmazható értékének meghatározásához célszerű egy terhelési tényezőt definiálni a következőképpen:

$$S = \frac{\text{tényleges terhelés}}{\text{maximális terhelhetőség } 25\ C^{o} - \text{on}}$$

A gyorsítási függvények csak adott stresszor tartományban érvényesek, mivel egy határérték felett azonnal tönkre megy az elem, egy adott érték alatt viszont nem javul tovább a meghibásodási tényező, amint azt a következő 6-2. ábra mutatja.



6-2. ábra: Gyorsítási tényező gyakorlati alakulása

6.3. Az emberi megbízhatóságot befolyásoló tényezők

Az ember-gép rendszerek megbízhatóság szempontjából fontos eleme a folyamatban résztvevő ember. A rendszerek kialakítása során az emberi

tényezők figyelembevételével külön tudomány, az ergonómia foglalkozik. Ezek részletkérdéseit nem kívánjuk taglalni, de röviden összefoglaljuk az ember megbízhatóságát befolyásoló tényezőket és az emberre jellemző megbízhatósági jellemzők alakulását.

Az ember munkavégzése során bekövetkező hiba valószínűsége több tényezőtől függ, ilyenek

- az ember képességei, készségei, valamint tulajdonságai,
- a tevékenységi környezet konkrét feltételei (az embert érő környezeti hatások),
- a mindenkori tevékenység jellege.

A következőkben ezeket a tényezőket vesszük szemügyre.

A biztonságkritikus rendszerekben tevékenykedő ember megfelelő megbízhatósága **képesség** oldaláról a megfelelő alkalmassági feltételek előírásával, **készség**ek oldaláról pedig megfelelő oktatással érhető el.

Az ember-gép rendszerben az embert érő fontosabb környezeti hatások

1. világítás,
2. zaj,
3. vibráció,
4. klíma,
5. kémiai anyagok,
6. pszicho-szociális tényezők.

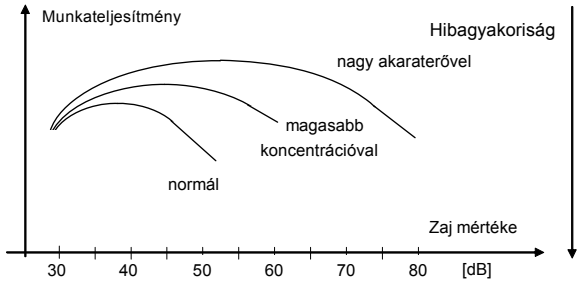
Nézzük röviden e hatásokat külön-külön.

1. Világítás

A munkahely megvilágítása döntően befolyásolja az ember hangulatát, munkavégző képességét, ezen keresztül megbízhatóságát. Az irodalom alapján a megvilágítás függvényében a következő ábrán jól látható módon: csökkenő megvilágítás mellett a munka bonyolultságától függően eltérő mértékben, de növekszik a hibagyakoriság.

2. Zaj

A zajok bizonyos mértékig aktivizáló hatásúak is lehetnek az emberi munkavégzésre. Újszerű, nem várt és erős zajok különös mértékben jutnak az ember tudatába – különös figyelmet ébresztenek. Bizonyos intenzitás feletti zaj esetén viszont már sérül a figyelem és koncentráció és a hibagyakoriság növekedéséhez vezet (6-3. ábra).



6-3. ábra A környezeti zaj és a hibagyakoriság minőségi összefüggése

3. Vibráció

Az emberi szervezet jellegzetessége, hogy nincs külön érzékszervünk a rezgések érzékelésére, ezért a rezgések hatása csak az egyéb érzékszervek észlelése alapján írható le. Az emberi test sok belső szerve egymástól független mozgásra képes, így ebből a szempontból a szervezet egy több tömegű rezgő rendszernek fogható fel, melynek rezonancia-frekvenciája a 10–100 Hz tartományban van. Az ilyen frekvenciájú rezgések rendkívül kellemetlenek a szervezetre. A hatás függ a frekvencián túl a rezgés amplitúdójától és a hatás időtartamától. A zavaró hatás elkerülésére a rezgés lehetőleg rövid ideig és kis amplitúdóval jelentkezzen. A sztochasztikus, rendszertelen rezgés fárasztóbb, mint a szabályos.

4. Klíma

Klíma alatt értjük az emberi szervezet és környezete közötti hőcserét befolyásoló tényezők összességét:

- száraz levegő hőmérséklete,
- légnedvesség (páratartalom),
- mozgó levegő sebessége,
- hősugárzás.

A klíma és az emberi teljesítmény szoros kapcsolatban van egymással. A részletes munka- és sport-fiziológiai vizsgálatok az ember fizikai és pszichológiai teljesítőképessége és a klimatikus hatások között az alábbi hatásokat mutatták ki:

A hőmérséklet növekedésével az emberi teljesítőképesség általában csökken, az emberi munkára jellemző meghibásodási ráta értéke feltétlenül

növekszik. ϑ>27 C° esetén λ növekedése már észrevehető mértékű, ϑ>30 C° esetén pedig a teljesítmény csökkenése is jelentős:

- a teljesítmény csökkenés mértéke függ a motivációtól: erősebb motiváció esetén a csökkenés kisebb, az erősebb motiváció a teljesítménytartalékok felhasználását elősegíti, de ebben az esetben tartós terhelésnél számolni kell a kimerülés veszélyével,
- erős klímaterhelés különösen kötött, szoros időrendben végzendő tevékenység esetén kedvezőtlen.

5. Kémiai anyagok

Kémiai anyagok jelenléte csak speciális esetben jelent stressz-tényezőt, ha az ember különböző vegyi-anyagokkal kerül kapcsolatba

- gázok,
- gőzök,
- por és
- folyadék.

A stressz-hatást befolyásoló tényezők lehetnek

- az anyag fajtája,
- az emberrel kialakult kapcsolat mértéke,
- az anyag koncentrációja,
- a hőmérséklet,
- a hatás időtartama,
- az ember egyéni érzékenysége.

6. Pszicho-szociális tényezők

A stressz kiváltó tényezői fizikai, pszichológiai, mentális, szociális hatások lehetnek.

- **Fizikai stresszor**nak tekinthető az érzékszervek túlzott igénybevétele vagy az emberi szervezet felől jelentkező kedvezőtlen visszacsatolás.
- **Pszichológiai stresszor**-ként különböző foglalkozási nehézségek jelentkezhetnek (mint például üzemi légkör, konfliktus munkatársakkal, főnökkel, megfelelő bérezés vagy megbecsültség hiánya, karrier törekvések, presztízs problémák stb.
- **Mentális stresszor**-t jelenthetnek a közreműködő emberrel szemben támasztott túlzott követelmények (akár a felfogó képességgel, akár a

döntési képességgel vagy a hosszúidejű memóriában tárolt tapasztalatok felhasználásával szemben).

- **Szociális stresszor**-t jelentenek a magán élet hatásai, vagy az ember helyzetéből adódó hatások (például az ember rangja stb.).

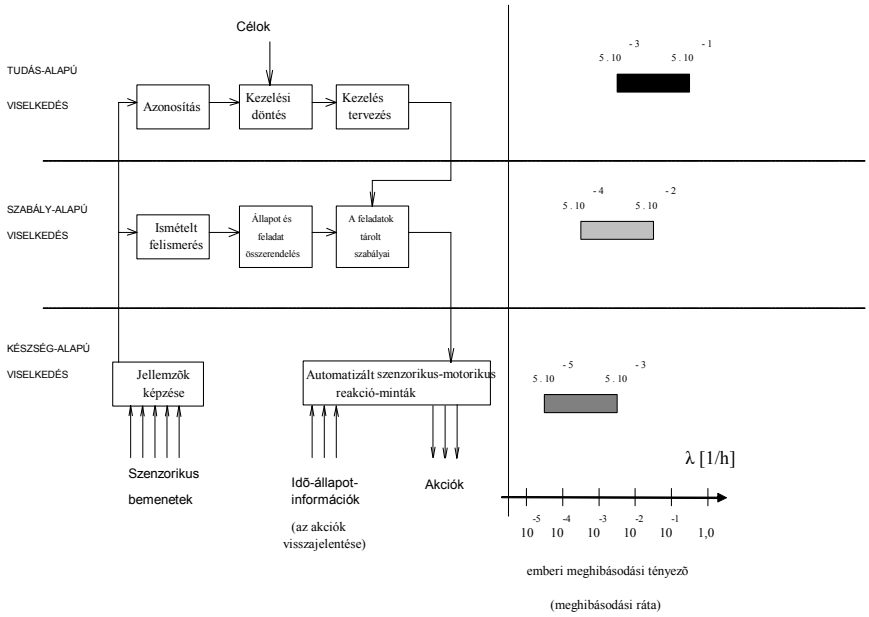
Látható, hogy az ember-gép rendszerek megbízható működését messze nemcsak műszaki, hanem pszichológiai és egyéb tényezők is jelentősen befolyásolják. Figyelembe kell venni, hogy az emberi hiba elkövetésének valószínűsége fenti környezeti hatások mellett nagymértékben függ a tevékenykedő embert érő stressz-hatásoktól és időfeltételektől is.

Végül az emberi tevékenység jellege is jelentősen befolyásolja a megbízhatóságot. Az ember-gép rendszerben tevékenykedő ember információ-feldolgozó tevékenysége során elkövetett hibák elemzésekor célszerű a tevékenység jellegét is figyelembe vevő számértékeket alkalmazni. Az ergonómiai irodalomban az ún. Rasmussen-féle 3-síkú tevékenységi modellt szokás alkalmazni, amely szerint a **készség, szabály és tudás alapú tevékenység** során eltérő az ember hibagyakorisága (6-4. ábra).

Az emberi megbízhatóságot befolyásoló tényezők áttekintése után fontos kérdés, hogyan alakul a számjellemzők értéke a tárgyalt befolyásoló tényezők függvényében. A megbízhatósági számjellemzők értékét vizsgálva durva közelítésként gyakran találkozunk az irodalomban egy $\lambda=10^{-3}$ [1/ó] átlagos értékkel. E szerint az ember megbízhatósága nagyságrendekkel kisebb, mint a műszaki eszközöké általában. Ez azonban nagyon sommás kijelentés, a biztonságelméleti szakirodalomban számos más adat is előfordul. A meghibásodási ráta megadásánál feltétlenül tisztázni kell, milyen tevékenységre vonatkozóan kívánjuk a meghibásodási ráta értékét meghatározni, illetve milyen körülmények között érvényesek az adott értékek.

Az adatok forrása:

- munkahelyi mérések,
- tesztek és szimulációs vizsgálatok (laboratórium!),
- baleseti- és zavar-statisztikák,
- szakértői becslések a nem mért közbenső értékekre vonatkozóan.



6-4. ábra: Az emberi információ-feldolgozás 3-síkú modellje (Rasmussen)

Az adatállományok a tevékenységeket különböző mélységben osztják fel elemeikre (esetenként „molekuláris" tevékenységelemekre). Adott esetben ezekből az elemekből kell a teljes tevékenységre vonatkozó meghibásodási rátát meghatározni.

A tevékenységelemekre bontásból természetesen számos probléma adódik:

- az adatok csak akkor érvényesek, ha ugyanolyan körülmények között végzik a tevékenységet,
- a meghibásodási ráta meghatározása óta változott a technológia, a berendezés – adatokat illeszteni kell az új körülményekhez,
- a meghibásodási rátát meghatározó tényezők nagyon összetettek,
- az ember nem funkcionálisan, hanem célirányosan cselekszik – egyes lépések hibás volta esetén is lehet hibátlan a teljes tevékenység.

A korábbi 6-4. ábra tartalmazta az egyes tevékenységi-körökre érvényes hibaráta értékeket is. Láthatóan a rutin jellegű feladatokat oldja meg az ember a legmegbízhatóbban és a tudás alapú tevékenységnél jelentkezik leggyakrabban hiba. A hibagyakoriságot befolyásoló tényezők függ-

vényében alakuló számjellemzőket a következő táblázatokban foglalhatjuk össze.

A környezeti feltételek két szélsőséges értékét tekintetbe véve adódó hibaráta értékek a 6-2. táblázatban láthatók.

Tevékenység jellege	λ[1/h] Környezeti feltételek	
	kedvező	kedvezőtlen
Készség alapú	$1 \cdot 10^{-3}$	$5 \cdot 10^{-3}$
Szabály alapú	$1 \cdot 10^{-2}$	$5 \cdot 10^{-2}$
Tudás alapú	$1 \cdot 10^{-1}$	$5 \cdot 10^{-1}$

6-2. táblázat: Emberi hibaráta értékek a környezeti feltételek függvényében

Az emberi hibatényező alakulását alapvetően befolyásolja az ember terhelésének mértéke. Ezt a következő szorzótényezőkkel lehet számításba venni a stressz-szint függvényében (6-3. táblázat):

Tevékenység jellege	Szorzótényező	
	alulterhelt	túlterhelt
Készség alapú	2	2
Szabály alapú	2	2
Tudás alapú	2	5

6-3. táblázat: Terhelési tényező a különböző tevékenységi körök esetén

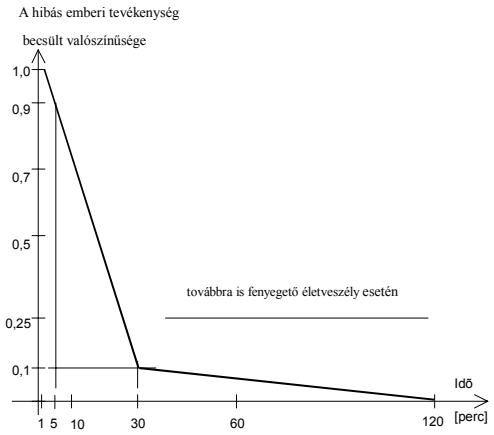
A fentiek alapján az ember hibatényezőjének számításba vételekor a javasolt értékek különböző feltételek mellett a következők (6-4. táblázat).

A fenti szokásos körülményekre érvényes számjellemzők mellett érdekességként megemlíthető egy amerikai atomerőmű-biztonsági publikációkban szereplő vizsgálati eredmény. Eszerint például atomerőművek katasztrofális meghibásodása esetén az emberi döntés hibavalószínűsége megközelíti az 1 értéket, amint azt a következő 6-5. ábra mutatja.

Az ábrából következik, hogy egy ilyen atomerőművi probléma esetén a meghibásodás jelentkezése után kb. 30 percen belül semmi kezelési tevékenységet nem szabad az emberre bízni, vagyis feltétlenül automatizált beavatkozás szükséges.

Tevékenység jellege	λ[1/h] Környezeti feltételek					
	kedvező			kedvezőtlen		
	alul terhelt	optimálisan terhelt	túl terhelt	alul terhelt	optimálisan terhelt	túl terhelt
Készség alapú	$2 \cdot 10^{-3}$	$1 \cdot 10^{-3}$	$2 \cdot 10^{-3}$	$1 \cdot 10^{-2}$	$5 \cdot 10^{-3}$	$1 \cdot 10^{-2}$
Szabály alapú	$2 \cdot 10^{-2}$	$1 \cdot 10^{-2}$	$2 \cdot 10^{-2}$	$1 \cdot 10^{-1}$	$5 \cdot 10^{-2}$	$1 \cdot 10^{-1}$
Tudás alapú	$2 \cdot 10^{-1}$	$1 \cdot 10^{-1}$	$2 \cdot 10^{-1}$	1	$5 \cdot 10^{-1}$	1

6-4. táblázat: Emberi tevékenység λ értékeinek összefoglaló táblázata



6-5. ábra: A hibavalószínűség alakulása az életet fenyegető veszélyeztetés esetén

Az emberek által elkövetett hibák kérdésével a minőségbiztosítási fejezetben még egyszer fogunk foglalkozni a minőséggel kapcsolatos költségek elemzése során (10.2. fejezet). Annyit azonban már itt is előrebocsáthatunk, hogy a hibákat ugyan az ember követi el, de ezek mélyebb oka általában a kialakított rendszerben keresendő. Deming fogalmazta meg ezt úgy, hogy a minőség javítása érdekében nem az embert kell megváltoztatni, hanem a rendszert.

7. A rendszerek megbízhatóságának modellezése

7.1. Rendszerekről általában

7.1.1. A rendszer fogalma

Rendszernek nevezzük adott feladatok teljesítésére egymással funkcionális kapcsolatban lévő elemek, alkatrészek egységét. A **megbízhatóság** – mint láttuk – **a feladat teljesíthetőségének valószínűsége.** A feladatok viszont a követelményekhez, körülményekhez illeszkedően rendszerint az időben nem állandóak. Elvileg lehetséges a megbízhatóságot dinamikusan értelmezni, figyelembe véve az egyes feladatok teljesítésének szükségességét, gyakoriságát. (A ritkábban adódó feladatokat teljesítő részek meghibásodási tényezőjét kisebb súllyal számításba véve, mint a folyamatosan adódó feladatokét.)

A megbízhatóság ilyen dinamikus értelmezése az üzemi viszonyokra reálisabb eredményeket szolgáltatna, mint a statikus, de csak adott típusú felhasználásra átlagosan lenne érvényes és nem az objektum specifikációjára. Ezért alapértelmezésként statikus analízist kell alkalmazni, amikor a rendszer készségét a specifikáció szerinti folytonosan teljesítendő valamennyi feladatára értelmezzük. Persze adott felhasználásban figyelembe lehet venni ezeket a körülményeket (lásd a kvázi redundanciára vonatkozó fejezetet).

A rendszerek általában túlzottan bonyolultak ahhoz, hogy teljességükben vizsgálva valamennyi kisebb hatású befolyásoló tényezőt is figyelembe vegyünk. Egyes tényezők elhanyagolhatóan csekély hatása a mérnöki munkában igen gyakran egyszerűsítéseket tesz lehetővé és szükségessé. Ezért ezúttal is egy modellt hozunk létre, amely egyszerűbb, kezelhető és azt analizáljuk. A megbízhatósági analíziskor elsősorban strukturális modellek alkalmazására lesz szükségünk.

A megbízhatóság szempontjából két lényegesen eltérő struktúrát különböztetünk meg: a redundancia mentest és a redundánsat.

7.1.2. Redundancia, redundáns rendszerek

A redundancia mentes objektumokban bármely rész meghibásodása a rendszer üzemképtelenségét eredményezi. A redundancia esetünkben a megbízhatóság növelését szolgáló többletet jelenti. Ez a többlet különbö-

ző célok érdekében építendő a rendszerbe, eszerint többféle redundanciáról beszélhetünk.

Funkcionális redundanciáról beszélünk, ha az objektumban egynél több lehetőség van adott funkció(k) teljesítésére. Ilyen redundanciát hardver és szoftver úton lehet létrehozni.

- A **hardver redundancia** megvalósításának módjai:
  - **Strukturális redundancia:** ekkor az objektumban adott funkció teljesítésére a minimálisan szükségesnél több egység (alkatrész) van, amelyek meghibásodás esetén biztosíthatják az adott funkció teljesítését.
  - **Igénybevételi redundancia:** ekkor az objektum egyes elemei képesek arra, hogy az alkalmazás során előadódó maximálisnál nagyobb funkcionális és/vagy környezeti terhelést viseljenek el meghibásodás nélkül, mert ezáltal a megbízhatóság általában nő. A szükségesnél nagyobb megengedhető terhelés elviselésére való méretezés az *aláterhelés* vagy **derating.** Az ebből adódó megbízhatóság növekedés a stresszre vonatkozó összefüggések (6.1. fejezet) segítségével határozható meg, például, ha az eszköznek a rá vonatkozó névleges hőmérsékletnél, feszültségnél kisebb a legnagyobb igénybevétele.
  - **Tolerancia redundancia:** Ebben az esetben a redundáns elem paramétereinek toleranciája kisebb, mint ami az adott alkalmazásban szükséges lenne. Például ±5%-os ellenállást építenek be egy olyan áramkörbe, amelyik hiba nélkül működne az ellenállás értékének akár ±20% eltérése esetén is. Emiatt az adott alkatrész meghibásodási tényezője kisebb lesz a katalógusában specifikált névleges értéknél. A javulás mértékét azonban csak abban az esetben lehet számításba venni, ha erre vonatkozó adat rendelkezésre áll. Mivel ez igen ritka, gyakorlatilag ezt a redundanciát csak a megbízhatósági tartalékok javára lehet írni.
- A **szoftver redundancia:** A szoftver is sok lehetőséget ad redundancia kialakítására. Ilyenek
  - a paritás vizsgálat,
  - a „kontrollszumma”,
  - a „watch-dog”,
  - a műveletek megismétlése és
  - az eredményeik összevetése stb.

Ezekkel a szoftver-megoldásokkal a hardver hibák hatása csökkenthető, a tranziens hibák esetleg teljesen kivédhetők. Mindezeket a megbízhatósági számítások során figyelembe vehetjük oly módon, hogy a szoftvert hibátlannak tekintjük. Más kérdést jelentenek viszont a szoftverben bennmaradt hibák kivédésére szolgáló megoldások, ezekkel nem foglalkozunk.

7.1.3. A redundancia mértéke

A **redundancia mértékére** egy lehetséges – főleg folyamatirányító rendszerekre értelmezett – kategorizálás:

1 hiba esetén:	korlátlan továbbműködés (fault tolerant)
	korlátozott továbbműködés (fail soft)
	tervszerű leállás (fail safe)
	riasztás és továbbműködés
2 hiba esetén lehet	fail soft, ami 1 hibánál fault tolerant stb., vagy
	fail safe, ami 1 hibánál fail soft.

7.1.4. Diverzitás

Bonyolultabb rendszerek esetén a redundancia speciális formájaként beszélhetünk a diverzitásról (kétcsatornás biztonsági rendszerek bizonyos megoldásainál, majoritás logikák esetén stb.)

A **diverzitás** szó szerint különbözőséget jelent – esetleg a legkisebb részletekig. A műszaki gyakorlatban nagyon sokféle diverziter megoldással találkozhatunk, melyek éppen a különbözőség mértékében, mélységében térnek el egymástól. E különbözőségnek nagy szerepe van a biztonsági rendszerek kialakításában, a hibafelismerésben stb.

A diverzitás megvalósítására számos lehetőség adódik ([14]):

- **Alkalmazási feltételek diverzitása:** egyetlen egység többszöri, különböző alkalmazását jelenti (például időbeli redundanciaként), segítségével a véletlenszerű hardver-meghibásodások felismerhetők.
- **Fizikai diverzitás:** két azonos egység alkalmazását jelenti, amelyek azonban a gyártási szórásból adódóan bizonyos mértékig különbözők. Ezzel a diverzitással véletlen és statikus hardvermeghibásodások ismerhetők fel.
- **Implementációs diverzitás:** a különböző feldolgozási utak ugyanazt a funkciót teljesítik, de más módon megvalósítva, segítségével felismerhetők az előbbi meghibásodásokon kívül az ún. implementációs hibák is. Az implementációs diverzitás realizációjának lehetséges módjai:

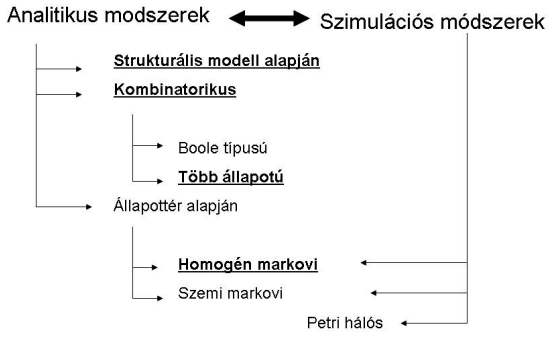
- különböző alkatrészek, integrált áramkörök
- különböző kapcsolás az áramköri egységben
- különböző részrendszerek (eltérő áramköri egységek)
- különböző mikroprogramok
- különböző operációs- és futasidő rendszerek
- különböző algoritmusok,
- különböző eljárások,
- különböző adatformátumok,
- különböző fordító programok (compiler),
- különböző programnyelvek,
- különböző programozási módszerek,
- különböző szoftver-eszközök,
- különböző teszt módszerek.

- **Funkcionális diverzitás**: A különböző feldolgozási utak különböző funkciókat valósítanak meg: a kimeneti értékeket nem összehasonlítják, hanem bizonyos összefüggéseket kell ellenőrizni. Felismerhetők segítségével az eddigi hibákon kívül a valódi funkcionális hibák, tervezési, specifikációs stb. hibák is.

7.2. A rendszerek vizsgálata során alkalmazott modellek

7.2.1. A rendszerek vizsgálatának általános módszerei

Az előzőekben áttekintettük, hogy milyen feladatok merülnek fel a rendszerek vizsgálata során, fontos azt is látni, milyen apparátus áll rendelkezésünkre a megoldás során. A lehetséges eljárásokat röviden számba véve egy lehetséges felosztás következőképpen alakul:



7-1. ábra: Megbízhatóság vizsgálat lehetséges módszerei

7.2.2. Struktúrán alapuló megbízhatóság-elemzés

Ha valamely termék megbízhatóságát a funkcionális és a konstrukciós struktúra alapján létrehozott megbízhatósági modell segítségével vizsgáljuk, akkor az egyes részek (részrendszerek, egységek, elemek) megbízhatósági adataiból számítjuk az eredő paramétereket. A rendszer elemeinek állapota határozza meg a rendszer állapotát. Az elemek és a rendszer állapota közötti összefüggést a rendszerfüggvény írja le, aminek általános formája a következő:

$$Y = f(\underline{X})$$

ahol

- Y – a rendszer állapotindexe,
- $\underline{X}$ – az elemek állapotindexeiből felépített vektor.

N elem esetén:

$$\underline{X}^T = \left[x_1, x_2, x_3, ..., x_i, ...x_N\right] \qquad (7\text{-}1)$$

A képletben az $\mathbf{x}_i$ az i-ik elemhez tartozó állapotindex, ami egy-egy bináris számmal írható le.

A rendszert alkotó egységek meghibásodási és javítási folyamatai (állapotváltozásai és állapotai) lehetnek egymástól **függetlenek,** de lehetnek ok-okozati kapcsolatban lévő **függőek.** A függetlenség a számítást jelentősen egyszerűsíti, mivel egyes eseményekhez tartozó valószínűségek összeszorozhatók, függés esetén viszont nem.

A **meghibásodási folyamat**okban nemcsak a másodlagos (meghibásodás okozta) meghibásodások esetén van függés. Egyes részek terhelését – és ezzel a meghibásodási tényezőjét – befolyásolhatja másik részek állapota. Például egy redundáns rendszerben a tartalék egység nincs terhelve mindaddig, amíg az elsődlegesen üzemelő jó, annak meghibásodásától a tartalék teljes terheléssel üzemel és ezért megnő a meghibásodási tényezője.

A **javítási folyamatok** is lehetnek egymástól függőek és függetlenek. A konstrukciósan összetartozó részek hibaelhárítását egyszerre végzik. Egy kártyán lévő két hibás alkatrészt nem szoktak egymástól függetlenül kicserélni. A javítási folyamatok olyan helyileg elkülönülten telepített egységek esetében függetlenek, ahol a javító személyzetek is egymástól távol vannak, vagy legalább is többen egymástól függetlenül dolgoznak.

A függés-függetlenség kérdését tehát mindenképpen tisztázni kell a számításokhoz.

7.3. A megbízhatóság vizsgálata a Boole-modell alapján

7.3.1. A modell alkalmazásának feltételei

Mint azt korábban már tárgyaltuk, igen gyakran csak kétféle minőségi állapotot értelmezünk:

up ≡ üzemképes ≡ jó ⇔ down ≡ üzemképtelen ≡ rossz.

Az indikátor ekkor mind az egyes elemekre, mind a rendszerre vonatkozóan csak kétféle értéket vehet fel. Ez a két érték önkényes, de célszerű választással:

up: x = 1, **down: x = 0.**

Az egyszerűbb írás kedvéért, ha nem kell külön hangsúlyozni, vagy az időben állandó, elhagyjuk az időfüggés jelölését. Általában azonban az indikátor időfüggvény. Az **x(t) = 1** állítás az **x** elem működőképességét jelenti a **t** időpontban, az **x = 1** állítás az **x** elem működőképességét általában.

A Boole modell szerint tehát valamennyi egységre, így például a **k**-adikra is: $x_k \in \{1, 0\}$, de az egységekből felépülő rendszerre is: $Y \in \{1, 0\}$. Ez a választás azért is kedvező, mert így az állapotváltozó egyben logikai értéket is képviselhet:

1 = igen , 0 = nem

Ha logikai függvényben alkalmazzuk, (ahol $\wedge$ a **logikai ÉS-,** a $\vee$ pedig a **logikai VAGY**-kapcsolatot jelenti), akkor $x_1 \wedge x_2$ tehát azt jelenti, hogy **x_1 és x_2** (mindkettő) jó, $x_3 \vee x_4$ pedig azt, hogy **x_3 vagy x_4** (legalább az egyik) jó.

A Boole modell alkalmazásának fontos feltételei a következők:

- a vizsgált elemek száma véges legyen,
- a vizsgált elemek csak két állapotot vegyenek fel, s végül
- teljesüljenek az ún. **monotónia feltétel**ek.

A monotónia feltétel tehát azt jelenti, hogy a rendszer állapotát egy meghibásodás nem javíthatja, tehát csak ronthatja, vagy változatlanul hagyhatja. Másképp fogalmazva: az elemek meghibásodása nem növelheti a rendszer megbízhatóságát és nem csökkentheti a javítási igényt.

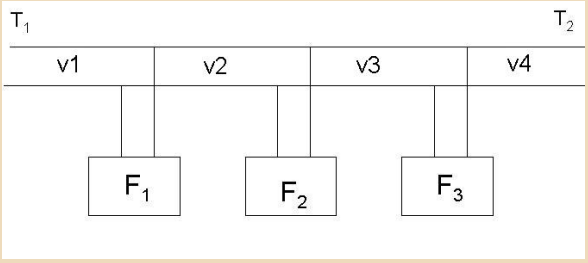
Részletesebben kifejtve a következő feltételeknek kell teljesülni:

1. Ha a rendszer minden eleme jó, akkor a rendszer is csak jó lehet (ezzel a tervezési hibát zárjuk ki). Matematikai formában e feltétel így írható: **Y=1**, ha $\forall k$-ra : $x_k = 1$.
2. Ha a rendszer valamennyi eleme rossz, nem lehet a rendszer jó (ezzel a csodákat zártuk ki). Matematikai formában: **Y= 0**, ha $\forall k$-ra : $x_k = 0$.
3. Ha egy üzemképtelen rendszer újabb eleme meghibásodik, akkor ettől nem kerülhet a rendszer ismét üzemképes állapotba (más szavakkal: egy meghibásodástól nem „javulhat meg" a rendszer).
4. Ha egy üzemképes rendszer meghibásodott elemét helyreállítják, akkor ettől nem kerülhet a rendszer üzemképtelen állapotba (más szavakkal: javítástól nem „romolhat el" a rendszer).

A monotónia feltételeket általában műszakilag ésszerűtlen feladatkitűzés, a műszaki rendszer meg nem felelő kialakítása, általában tehát specifikációs-, tervezési- és gyártási hibák sértheti meg. Ezek illusztrálásaként tekintsük a következő egyszerű példát:

7-1. példa:

Három felhasználót (F_1, F_2, F_3) táplálunk két betápláláson (T_1, T_2) keresztül (ún. körvezeték), a v_1, v_2, v_3 és v_4 vezetékek segítségével a következő 7-2. ábra szerint.



7-2. ábra: Példa nem monoton rendszerre

Ebben a példában tekintsük csak a 3. felhasználót. Ez például lehet egy ipari üzem. Rendszer-meghibásodásnak tekintjük a feszültségnek a 3. felhasználónál egy bizonyos előre meghatározott határ alá történő lecsökkenését. Tételezzük fel, hogy az 1. betáplálás meghibásodik és valamennyi felhasználót a 2. betápláláson keresztül táplálják. A terhelés és ezzel a feszültségesés a 4. vezetéken, mivel ezen folyik valamennyi felhasználói áram, olyan nagy, hogy a 3. felhasználónál a feszültség az előírt normál érték alá csökken, és így a rendszert üzemképtelennek kell tekinteni. Ha most még a 3. vezeték is meghibásodik, akkor a 4. vezeték terhelése ismét lecsökken és a 3. felhasználónál a feszültség ismét megnövekszik, úgy hogy a rendszer ismét üzemképes lesz. Ebben az esetben a 3. monotónia feltétel nem fog teljesülni.

A fenti példában a monotónia-feltételek nem teljesülését a körvezeték meg nem felelő kialakítására vezethetjük vissza, tehát azt mondhatjuk, hogy a monotónia-feltételek akkor is megsérülhetnek, ha az elemek meghibásodása esetén bizonyos önszabályozó hatások lépnek fel.

A rendszert alkotó egységek állapotait leíró $\mathbf{X^T}$ indikátor bináris vektort alkot. Például $\mathbf{X^T(t) = [1, 1, 1, 0, 1]}$ egy olyan ötegységes rendszer vektora, amelyiknek a t időpontban a negyedik eleme rossz, a többi jó. Azt, hogy $\mathbf{Y(t)}$ ebben az esetben **1** vagy **0,** azt a rendszerfüggvény alapján határozhatjuk meg.

Az **N** egységből felépített rendszer egységeinek állapotai egy nullákat és egyeseket tartalmazó **N** jegyű kettes számrendszerbeli számként is megjeleníthető. Ezzel egyes esetekben az egyenlőtlenségi relációk – < és > – is értelmezhetők monoton rendszerekre.

A Boole modellben a rendszerfüggvényre érvényes, hogy **x** várható értéke megegyezik az x = 1 valószínűségével, vagyis

$$M\{x\} = \Pr\{x = 1\}$$

Bizonyítás:

$$M\{x\} = 1 \cdot \Pr\{x = 1\} + 0 \cdot \Pr\{x = 0\} = \Pr\{x = 1\} \qquad (7\text{-}2)$$

A Boole modell érvényessége esetén a rendszerfüggvény Boole függvény. Például vizsgáljunk egy olyan háromegységes rendszert, amely akkor működőképes, ha az összes eleme jó (a következő fejezetben látni fogjuk,

hogy az ilyen rendszert megbízhatósági szempontból soros rendszernek tekinthető). Az ezt leíró Boole függvény:

$$Y_S = 1, \text{ ha } (x_1 = 1) \wedge (x_2 = 1) \wedge (x_3 = 1) \tag{7-3}$$

Vegyük észre, hogy az

$$Y_S = x_1 \cdot x_2 \cdot x_3 \tag{7-4}$$

összefüggés is igaz. Ez az írásmód egyben számítási eljárást is ad. Mindez az indexek önkényes, de láthatóan igen célszerű megválasztásának kedvező következménye.

A Boole típusú rendszerfüggvény bemutatására egy másik példa lehet egy olyan két-egységes rendszer, amelyik akkor működőképes, ha legalább az egyik eleme jó. Az ilyen (párhuzamos) rendszerre a függvény:

$$Y_P = 1, \text{ ha } (x_1 = 1) \vee (x_2 = 1) \tag{7-5}$$

Ebben az esetben a rendszerfüggvényt a soroshoz viszonyítva kevésbé egyszerű aritmetikai művelettel lehet átírni:

$$Y_P = 1 - (1 - x_1) \cdot (1 - x_2) \tag{7-6}$$

A Boole-modellel kezelhető egységek alaptípusai az előzőekben bemutatott soros és párhuzamos struktúrájú rendszerek és az ilyen struktúrájú részrendszerekből felépülő olyan nagyobb rendszerek, amelyek a részrendszerekből soros és/vagy párhuzamos struktúrával létrehozhatók. Az ilyen rendszereket a továbbiak során **kanonikus**nak nevezzük. A kanonikus struktúrákkal gyakran nagyobb rendszer részrendszereként találkozhatunk

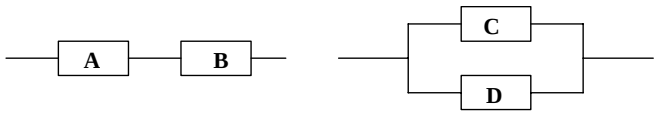
7.3.2. Kanonikus struktúrák vizsgálata

7.3.2.1. Általános megjegyzések

A megbízhatósági blokkdiagram alapján történő megbízhatóság-vizsgálat tipikus alkalmazási területe a kanonikus rendszerek vizsgálata. Ezek megbízhatósági analízise általában sokkal egyszerűbb mint az általános, bonyolultabb struktúráké. Ezért a rendszerek iteratív tervezése, fejlesztése során célszerű mint közelítést alkalmazni olymódon, hogy a feladatot az első lépésekben valamelyik kanonikus struktúrájú egyszerűbb modellel próbáljuk megoldani és a szükségnek megfelelően a tervezés további **finomítá-**

sakor folytatódhat a fejlesztés a későbbiek során tárgyalásra kerülő egyre bonyolultabb modellekkel.

A soros-párhuzamos megbízhatósági struktúrát a szokásos módon ábrázoljuk a megbízhatósági modellben. Ez az ábrázolás azonban semmiképpen nem áramköri kapcsolatot vagy funkcionális blokkdiagram szerinti „kaszkád–parallel" összeköttetést jelöl, hanem a megbízhatósági modellen alapuló logikai **„ÉS",** illetve **„VAGY"** kapcsolatra utal. A soros és párhuzamos rendszer megbízhatósági blokkdiagramját a következő 7-3. ábra mutatja:



7-3. ábra: Soros és párhuzamos rendszer megbízhatósági blokkdiagramja

A soros struktúra tipikus példája a kaszkádba (sorban egymás után) kapcsolt egységek (például jelfeldolgozó fokozatok) rendszere. Az ilyen elrendezés adta a „soros" elnevezést.

A funkcionális és a megbízhatósági struktúra gyakran eltérő. Például egy sínrendszerű elrendezésben az egységek a funkcióktól, hibakritériumtól függően lehetnek akár soros, akár párhuzamos megbízhatósági struktúrájúak. Vagy például két párhuzamosan kötött kapcsoló érintkezői párhuzamos struktúrát alkotnak; ha csak olyan hibájuk létezik, hogy nem hoznak létre összeköttetést bekapcsolt állapotban, míg ugyanez a kapcsoló-pár soros struktúrájú, ha csak olyan hibájuk lehet, hogy nem képesek kikapcsolni (beragadnak). Ha egyik hibafajta sem zárható ki, akkor nem lehet a kanonikus modellt alkalmazni.

7.3.2.2. Soros rendszer

A legegyszerűbb és leggyakoribb kanonikus struktúra a soros. Az ilyen rendszer definíció szerűen akkor és csak akkor működőképes, ha valamennyi eleme működőképes. Egy **N** elemű rendszerre tehát:

$$Y_S = 1, \quad \text{ha} \quad (x_1 = 1) \wedge (x_2 = 1) \wedge (x_3 = 1) \wedge \ \ldots \wedge \ (x_N = 1) \qquad (7\text{-}7)$$

Vagyis a soros rendszer akkor jó, ha az első eleme jó **ÉS** a második eleme is jó **ÉS** a harmadik is és stb., azaz valamennyi jó. De a soros rendszer más módon is definiálható:

$$Y_S = 0, \quad \text{ha} \quad \exists\, i: \quad x_i = 0 \tag{7-8}$$

Vagyis a soros rendszer akkor működésképtelen, ha létezik olyan eleme, amelyik működésképtelen.

Az első definícióból adódóan – mint korábban már láttuk – ez még másképpen is írható:

$$Y_S = \prod_{i=1}^{N} x_i \tag{7-9}$$

Tehát az elemek állapotindexeinek összeszorzásával is megkaphatjuk a soros rendszer állapotindexét (hiszen ha csak egy zérus is van az elemek állapotindexei között, akkor a szorzat zérus lesz).

Ha az elemek függetlenek egymástól, (ha minden elemre érvényes az, hogy a meghibásodási tényezője nem függ egyetlen másik elem állapotától sem), akkor az állításokhoz tartozó valószínűségek összeszorzásával kaphatjuk a rendszerre vonatkozó eredő valószínűséget. A függetlenség nemcsak a meghibásodási, hanem a javítási folyamatokra is értelmezhető és ekkor az üzemképességek valószínűsége szorozható össze.

Ha a rendszer soros, az egységek egymástól független meghibásodásúak és nincs javítás, a rendszer hibamentes működésének valószínűsége az egységek hibamentessége valószínűségének szorzata (a soros rendszer megbízhatósági függvénye):

$$R_s(t) = \prod_{i=1}^{N} R_i(t) \tag{7-10}$$

Ha a rendszer **soros**, **van javítás** és az egységeknek nemcsak a meghibásodása, hanem a **javítása is független,** akkor a rendszer üzemképessége az egységekre vonatkozó értékek szorzataként számítható:

$$d_S(t) = \prod_{i=1}^{N} d_i(t) \tag{7-11}$$

Sőt az eredő $\mathbf{K_S}$ tartós üzemkészségre (készenléti tényezőre)

$$K_s = \prod_{i=1}^{N} K_i \tag{7-12}$$

Bizonyítás:

Az R(t) függvényekre felírva, de d(t)-re és K-ra is érvényes módon:

$$R_S(t) = \Pr\{Y_S(t)=1\} = \Pr\left\{\prod_{i=1}^{N}[x_i(t)=1]\right\} = \\ = \prod_{i=1}^{N}\left[\Pr\{x_i(t)=1\}\right] = \prod_{i=1}^{N} R_i(t) \tag{7-13}$$

Ha nincs javítás és a meghibásodási tényezők állandó értékűek, vagyis valamennyi $R_i(t)$ függvényre

$$R_i(t) = e^{-\lambda_i \cdot t} \tag{7-14}$$

akkor

$$R_s(t) = e^{-\lambda_s \cdot t} \quad \text{ahol} \quad \lambda_s = \sum_{i=1}^{N}\lambda_i \tag{7-15}$$

Bizonyítás:

Általánosan, időben változó meghibásodási tényezőre felírva:

$$R_i(t)=\exp\left[-\int_0^t \lambda_i(t)\,dt\right] \quad \text{és} \quad R_s(t)=\exp\left[-\int_0^t \lambda_s(t)\,dt\right] \tag{7-16}$$

Utóbbi alapján:

$$R_s(t) = \prod_i\left\{\exp\left[-\int_0^t \lambda_i(t)\cdot dt\right]\right\} = \exp\left[-\sum_i\int_0^t \lambda_i(t)\cdot dt\right] \tag{7-17}$$

Tehát

$$\lambda_s(t) = \sum_i \lambda_i(t) \tag{7-18}$$

Ha $\boldsymbol{\lambda_k(t) = \lambda_k}$ az időtől független állandó valamennyi **k**-ra, akkor $\boldsymbol{\lambda_S}$ is konstans:

$$\lambda_s = \sum_i \lambda_i \tag{7-19}$$

és így az első meghibásodásig várható jó működési idő:

$$T_{FS} = \frac{1}{\lambda_S} = \frac{1}{\sum_{i=1}^{N} \lambda_i} \qquad (7\text{-}20)$$

Ez az egyszerű képlet a megbízhatósági számítások gyakorlati alkalmazása során szinte a leggyakrabban használt összefüggés.

A konstans meghibásodási tényezők (ráták) összegzése során az állandóság tulajdonsága megmarad, így a nem öregedő alkatrészekből felépített soros rendszer is megőrzi ezt a nem öregedő tulajdonságot (a hibafa elemzés kapcsán e kérdésre a 7.3.6.1 fejezetben még visszatérünk).

Soros rendszer esetén az exponensek összeadhatóságának feltétele a valószínűségek összeszorozhatósága és az ehhez tartozó matematikailag elvileg szükséges feltétel a **függetlenség.** Bár a másodlagos meghibásodások nem független események, hanem korábbi meghibásodások következményei, a soros rendszer állapotát már nem befolyásolják, hiszen a soros rendszer bármelyik [egyetlen] elemének meghibásodása rendszerhibát okoz.

Minden tartalékolást, redundanciát nélkülöző készülék soros struktúrájú. A kommersz háztartási gépek, rádiók, TV-k, telefonkészülékek stb., tehát az elektronikai ipar egyszerűbb termékeinek megbízhatósága ezzel az egyszerű módszerrel számítható. A továbbiakban tárgyalt modellekkel összevetve látható lesz, hogy a soros struktúra rendszertechnikailag is, elméletileg is, a számítási apparátust illetően is a **legegyszerűbb** megbízhatósági modell. Ebben az esetben nem kell mást tenni, csak az aktuális meghibásodási tényezőket összegezni és ez az összeg a rendszer eredő meghibásodási tényezőjét adja, aminek reciprok értéke a rendszer várható jó működési ideje, sőt ha a javítás mindig teljes felújítás, akkor egyben a meghibásodások közötti jó működési idő várható értéke is.

Megjegyzés: A biztonságkritikus, **nagy-megbízhatóságú** berendezések általában tartalmaznak redundanciát, ezért a soros modell a megbízhatósági analízisükhöz közvetlenül **nem használható!**

Az ún. **nem „monoton" rendszerek** esetében előfordulhat, hogy egy újabb hiba javítja a rendszer állapotát, az ilyen rendszereket is másképpen kell modellezni, hiszen nem függetlenek eleműek.

A soros rendszerre vonatkozó összefüggések ismeretében megállapítható, hogy a rendszer eredő megbízhatósága mindig kisebb, mint az összetevők közül akár a legkisebb, hisz értéke 1-nél kisebb valószínűségek szorzataként adódik. Ugyancsak ebből a tényből következik, hogy a soros rendszer megbízhatóságának javítását mindig úgy célszerű végezni, hogy a legkisebb megbízhatóságú, vagy legnagyobb meghibásodási tényezővel rendelkező elemét kell jobbra cserélni. Ez az ún. **„leggyengébb láncszem”** elvének felel meg. A számszerű összefüggések alapján világos, hogy mindig a legrosszabb elem felelős az egész rendszer megbízhatóságáért.

7-2. példa:

Egy soros struktúrájú átviteli lánc öt egységből áll, ezek közül négynek a meghibásodási tényezője $\lambda = 1/T$, az ötödiké $k \cdot \lambda$.

a) Ha **k=1** (tehát az ötödik is egyforma a többivel), az első meghibásodásig várható jó működési idő:

$$T_F = \frac{1}{5 \cdot \lambda} = \frac{T}{5}$$

b) Ha **k=10** (tehát az egyik elem tízszer rosszabb a többinél), az idő kb. a harmadára romlik:

$$T_F' = \frac{1}{14 \cdot \lambda} = \frac{T}{14}$$

c) Ha viszont csak egyetlen eleme 10-szer erősebb a láncnak, az az egész láncot alig teszi erősebbé. Legyen **k=0,1** , ekkor az első meghibásodásig várható jó működési időben ez csak kb. 22%-os javulást eredményez:

$$T_F'' = \frac{1}{4,1 \cdot \lambda} \approx 1,22 \cdot T_F$$

A fentieket összefoglalva egy soros rendszer megbízhatósága jelentősen javítható, ha van olyan eleme, amelyiknek meghibásodási tényezője lényegesen nagyobb, mint a többi elemé és ezt az egyetlen elemet egy jobbra cseréljük. Viszont egyetlen az átlagosnál jobb elem alkalmazása nem biztos, hogy számottevő megbízhatóság javulást eredményez. Ismeretes az

ún. Pareto-elv túlzottan leegyszerűsített alkalmazása: eszerint az elemeknek a 20%-a határozza meg a rendszer eredő megbízhatóságának 80%-át. Ez persze általában nem igaz.

7-3. példa:

További példaként tekintsünk egy n tagú soros rendszert, melynek egymástól független részrendszerei különböző megbízhatóságúak. Ezek megbízhatóság függvénye R_1, R_2,..., R_n. Javítsuk úgy a rendszert, hogy minimális ráfordítás ellett eredő megbízhatósága a kiindulási x értékről növekedjék egy kívánt y értékre.

Jelölje az eredeti megbízhatóság értékeket x_i, a javított értékeket pedig y_i. Ekkor

$$x = x_1 \cdot x_2 \cdot \ldots \cdot x_n$$

Legyen y>x a fejlesztendő rendszer eredő megbízhatósága. Keressük a ráfordítás minimumát az

$$y = y_1 \cdot y_2 \cdot \ldots \cdot y_n = \prod_{i=1}^{n} (x_i + \varepsilon_i)$$

feltétel mellett.

Rögzített $x_i \le x_{i+1}$ értékek esetén a ráfordítás akkor minimális, ha a rendszer megbízhatóság szempontjából „egyenszilárdságú", ekkor a megbízhatóság-növekmények:

$$\varepsilon_i = \sqrt[j]{\frac{y}{x_{j+1} \cdot \ldots \cdot x_n}}$$

ahol $i = 1,2\ldots j$; és

$\varepsilon_{i+1} = \ldots = \varepsilon_n = 0$ és a

j indexet a $\nu_j < y \le \nu_{j+1}$ egyenlőtlenséggel lehet meghatározni és itt

$$\nu_{i+1} = \left(\frac{x_{i+1}}{x_i}\right)^i \cdot \nu_i \quad \text{és}$$

$$\nu_1 = x \quad \text{valamint} \quad x_{n+1} = 1$$

1. számpélda:

Ha valamely független soros rendszer részegységeinek megbízhatósága rendre:

$$x_1 = 0,983;\ x_2 = 0,986;\ x_3 = 0,987;\ x_4 = 0,991$$
$$x_5 = 0,995;\ x_6 = 0,997;\ x_7 = 0,998;\ x_8 = 0,999$$

akkor mennyivel növeljük az egyes megbízhatósági értékeket, ha minimális ráfordítás mellett y=0,974 eredő megbízhatóságot akarunk elérni?

Kidolgozás:

$$\nu_1 = \prod_{i=1}^{8} x_i \cong 0,9377 \qquad \nu_2 = \frac{x_2}{x_1} \cdot \nu_1 \cong 0,9405$$

$$\nu_3 = \left(\frac{x_3}{x_2}\right)^2 \cdot \nu_2 \cong 0,9424 \qquad \nu_4 = \left(\frac{x_4}{x_3}\right)^3 \cdot \nu_3 \cong 0,9539$$

$$\nu_5 = \left(\frac{x_5}{x_4}\right)^4 \cdot \nu_4 \cong 0,9694 \qquad \nu_6 = \left(\frac{x_6}{x_5}\right)^5 \cdot \nu_5 \cong 0,9792$$

$$\nu_5 < y < \nu_6, \quad \text{így } x_i + \varepsilon_i = \sqrt[5]{\frac{y}{x_6 x_7 x_8}} \cong 0,996$$

A szükséges növekmények pedig:

$$\varepsilon_1 = (x_i + \varepsilon_i) - x_1 \cong 0,996 - 0,983 = 0,013$$
$$\varepsilon_2 = (x_i + \varepsilon_i) - x_2 \cong 0,996 - 0,986 = 0,010$$
$$\varepsilon_3 = (x_i + \varepsilon_i) - x_3 \cong 0,996 - 0,987 = 0,009$$
$$\varepsilon_4 = (x_i + \varepsilon_i) - x_4 \cong 0,996 - 0,991 = 0,005$$
$$\varepsilon_5 = (x_i + \varepsilon_i) - x_5 \cong 0,996 - 0,995 = 0,001$$
$$\varepsilon_6 = \varepsilon_7 = \varepsilon_8 = 0$$

Vagyis az eredmény szerint a rendszer öt legkisebb megbízhatóságú elemét kell javítani, hogy a kívánt eredő megbízhatósági értéket elérjük.

2. számpélda:

Legyen egy független soros rendszer elemeinek megbízhatósága rendre

$$x_1 = 0,980 \quad x_2 = 0,985 \quad x_3 = 0,987 \quad x_4 = 0,994$$

akkor mennyivel kell növelnünk az egyes megbízhatósági értékeket, hogy ha minimális ráfordítás mellett y=0,98 eredő megbízhatóságot akarunk elérni?

Kidolgozás:

Minden egyes részegység megbízhatóságát növelni kell, hiszen $x_4 < \sqrt[4]{y} \cong 0,995$, tehát $\varepsilon_i = \sqrt[4]{y} - x_i$, vagyis

$$\varepsilon_1 = 0,015 \quad \varepsilon_2 = 0,010 \quad \varepsilon_3 = 0,008 \quad \varepsilon_4 = 0,001$$

7.3.2.3. Párhuzamos rendszer

A legegyszerűbb redundáns struktúra a párhuzamos, ennek a kanonikus struktúrának a definíciója:

$$Y_P = 1, \quad \text{ha} \quad \exists i: \; x_i = 1 \tag{7-21}$$

vagyis a párhuzamos rendszer mindaddig működőképes, amíg van legalább egy működőképes eleme. Egy **N** elemű rendszerre:

$$Y_P = 1, \quad \text{ha} \quad (x_1 = 1) \vee (x_2 = 1) \vee (x_3 = 1) \vee .. \vee (x_N = 1) \tag{7-22}$$

vagy

$$Y_P = 0, \quad \text{ha} \quad (x_1 = 0) \wedge (x_2 = 0) \wedge (x_3 = 0) \wedge .. \wedge (x_N = 0) \tag{7-23}$$

A párhuzamos rendszer **forrótartalékolt,** ha valamennyi még működőképes egysége folyamatosan működik, egyformán terhelt és az egységek egymástól függetlenül hibásodhatnak meg. Ezért forrótartalékolás esetén a függetlenség miatt:

$$F_P = 1 - R_P(t) = \prod_{i=1}^{N} [1 - R_i(t)] = \prod_{i=1}^{N} [F_i(t)] \tag{7-24}$$

Ha a rendszer **forrótartalékolt párhuzamos** és **nincs javítás,** a rendszer hibamentes működésének valószínűsége az egységek hibamentességének valószínűségéből számítható:

$$R_P(t) = 1 - \prod_{i=1}^{N} [1 - R_i(t)] \tag{7-25}$$

Ha a **forrótartalékolt párhuzamos** rendszerben **van javítás** és az egységeknek nemcsak a meghibásodása, hanem a **javítása is független,** akkor a rendszer üzemképessége az egységekre vonatkozó értékekből számítható:

$$d_P(t) = 1 - \prod_{i=1}^{N} [1 - d_i(t)] \tag{7-26}$$

Sőt az eredő K_P **készenléti tényező**re is érvényes:

$$K_P = 1 - \prod_{i=1}^{N} (1 - K_i) \tag{7-27}$$

Ha a forrótartalékolt párhuzamos rendszert alkotó egységek egyformák (ez nem ritka eset), akkor a szorzás hatványozássá egyszerűsödik:

$$\begin{aligned} R_P(t) &= 1 - [1 - R(t)]^N \\ d_P(t) &= 1 - [1 - d(t)]^N \\ K_P(t) &= 1 - [1 - K(t)]^N \end{aligned} \tag{7-28}$$

Például egy kétegységes párhuzamos rendszer esetén:

$$d(t) = 1 - [1 - d_1(t)] \cdot [1 - d_2(t)] = d_1(t) + d_2(t) - d_1(t) \cdot d_2(t) \tag{7-29}$$

Ha nincs javítás:

$$R_P(t) = R_1(t) + R_2(t) - R_1(t) \cdot R_2(t) \tag{7-30}$$

Ha pedig az egységek egyformák (ami a párhuzamos rendszerek esetében nem ritka):

$$R_1(t) \equiv R_2(t) \equiv R(t) \tag{7-31}$$

akkor

$$R_P(t) = 2R(t) - R^2(t) \tag{7-32}$$

A várható élettartam a (4-21) képlet alapján:

$$T_F^{(2)} = \int_0^\infty R_P(t)\,dt = \frac{1,5}{\lambda} \tag{7-33}$$

Bizonyítás:

$$T_F^{(2)} = \int_0^\infty \left[2R(t) - R^2(t)\right] dt = \int_0^\infty \left[2e^{-\lambda \cdot t} - e^{-2\lambda \cdot t}\right] dt = \\ = \frac{2}{\lambda} - \frac{1}{2\lambda} = \frac{3}{2\lambda} = \frac{1,5}{\lambda} \tag{7-34}$$

ahol a $T_F = 1/\lambda$ az egyetlen elem élettartama.

Láthatóan a redundancia miatt adódó nyereség időben csupán 50%, ennyivel nő az élettartam (a kétszeres költség ellenére).

Általában N egyforma λ meghibásodási tényezőjű egységből felépített párhuzamos rendszer esetén az első meghibásodásig várható élettartam,

$$T_F = \left(1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{N}\right) \cdot \frac{1}{\lambda} \tag{7-35}$$

Bizonyítás:

A korábbiak szerint

$$R_p(t) = 1 - F^n(t) \quad \text{ahol} \quad F(t) = 1\text{-}R(t) \tag{7-36}$$

A λ=állandó feltétel esetén:

$$\frac{dF(t)}{dt} = \lambda \cdot e^{-\lambda \cdot t} = \lambda \cdot \left[1 - F(t)\right] \tag{7-37}$$

amiből

$$dt = \frac{1}{\lambda \cdot \left[1 - F(t)\right]} dF(t) \tag{7-38}$$

Integrálás után:

$$T_F = \frac{1}{\lambda} \cdot \int \frac{1 - F^N}{1 - F} \cdot dF = \frac{1}{\lambda} \cdot \int_0^1 \sum_0^{N-1} F^i dF = \frac{1}{\lambda} \cdot \sum_{i=0}^{N-1} \frac{F^{i+1}}{i+1}\Bigg|_{F=0}^{F=1} = \frac{1}{\lambda} \cdot \sum_{i=1}^{N} \frac{F^i}{i}\Bigg|_{F=0}^{F=1} \tag{7-39}$$

vagyis tényleg:

$$T_F = \frac{1}{\lambda} \cdot \sum_{i=1}^{N} \frac{1}{i} \tag{7-40}$$

Vegyük észre, hogy párhuzamos struktúra (forró **tartalékolt párhuzamos** struktúra) esetén az egyforma egységek számának növekedésével **egyre kisebb mértékben nő a rendszer várható élettartama:** a második egység csak a saját várható jó működési idejének a felével, a harmadik csak a harmadával növeli az eredő időt. Ez persze nem jelenti azt, hogy a megbízhatóságot nem növeli a párhuzamos redundancia számottevően, az előnyök különösen rövid ideig működtetett vagy javított (karbantartott) rendszerekben mutatkoznak.

7-4. példa:

Négy egyforma forrótartalékolt párhuzamos egység részrendszert alkot. Mekkora a megbízhatóság és a meghibásodásig várható működési idő?

$$R_P^{(4)} = 1-(1-R)^4 = 1-(1-4R+6R^2-4R^3+R^4) = 4R-6R^2+4R^3-R^4$$

Ha tehát $R(t)=e^{-\lambda t}$, akkor

$$R_P^{(4)} = 4e^{-\lambda t}-6e^{-2\lambda t}+4e^{-3\lambda t}-e^{-4\lambda t}$$

Innen integrálással ugyanazt az eredményt kapjuk, mint a fenti képlettel:

$$T_{FP} = \frac{4}{\lambda}-\frac{6}{2\cdot\lambda}+\frac{4}{3\cdot\lambda}-\frac{1}{4\cdot\lambda} = \frac{25}{12\cdot\lambda} \quad \text{vagy másképpen}$$

$$T_{FP} = \frac{1}{\lambda}\left(1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}\right)$$

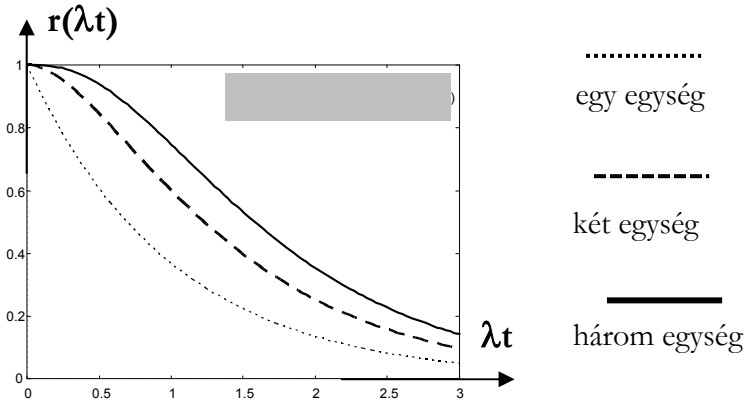
A 7-4. ábra mutatja az egy egységből álló redundancia mentes rendszer és a két és három egyforma egységet tartalmazó redundáns rendszer megbízhatóságának időfüggvényét. A vízszintes tengelyen az idő az egységek várható élettartamára normalizált.

Az ábrából is látható, hogy a párhuzamos tartalékolás előnye a rövid idejű alkalmazások esetében jelentős: minden egyes görbe vízszintes érintővel indul:

$$\frac{dR_P(t)}{dt} = 0 \qquad \text{ha} \qquad t=0 \tag{7-41}$$

Bizonyítás:

Fenti jellegzetesség két, illetve három elemből álló párhuzamos rendszerre könnyen igazolható módon teljesül:



7-4. ábra: Egy egység, illetve két és három párhuzamos forrótartalékolt egység megbízhatóságának időfüggvénye

$$\left.\frac{dR_P^{(2)}}{dt}\right|_{t=0} = \frac{d(2R-R^2)}{dt} = 2-2R\big|_{t=0} = 2-2=0$$

$$\left.\frac{dR_P^{(3)}}{dt}\right|_{t=0} = \frac{d(3R-3R^2+R^3)}{dt} = (3-6R+3R^2)\big|_{t=0} = 3-6+3=0$$

Ez azt jelenti, hogy ha $t \ll \frac{1}{\lambda}$, akkor első durva közelítéssel teljesen hibamentesnek vehető a rendszer. A rövid küldetési idejű berendezésekben, ahol a működési idő, kicsi, igen nagy megbízhatóság érhető el ezzel a struktúrával. Az állandó felügyelettel működtetett rendszerek esetében, ahol a megelőző karbantartások közötti idő kicsi: $T_{MK} \ll \frac{1}{\lambda}$, illetve ha a felügyeleti rendszer a hibát azonnal észleli és rövid idő alatt elhárítja, számíthatóan kis kockázattal üzemelhet a rendszer, illetve adott kockázathoz kiszámítható a TMK-k maximális időköze.

7-5. Példa:

A rendszert két egyforma, λ meghibásodási tényezőjű forrótartalékolt egység alkotja, a javítás tervszerű megelőző karbantartás, $\mathbf{T_{MK}}$ idő szerint periodikus. Számítsuk ki, milyen gyakran kell karbantartani (ellenőrizni és kicserélni az esetlegesen meghibásodott egységet), azaz mennyi lehet maximálisan a $\mathbf{T_{MK}}$ idő, ha a rendszer megbízhatósága nem csökkenhet egy

adott minimális határérték alá, vagy – más szóval – a rendszerhiba kockázata egy adott $F_{max}=1-R_{min}$ értéknél nem lehet nagyobb?

Megoldás:

Felhasználva a kétegységes forrótartalékolás megbízhatóságára rendelkezésünkre álló időfüggvényt:

$$R_P^{(2)} = 2 \cdot R - R^2 \qquad \text{ahol} \qquad R=e^{-\lambda \cdot T_{MK}}$$

A feladatban szereplő feltétel pedig:

$$R_p^{(2)} > R_{min} = 1 - F_{max}$$

Az R(t)-re vonatkozó másodfokú egyenletet megoldva az R valószínűségre egy lehetséges érték adódik:

$$R = 1 - \sqrt{1 - R_{min}} = 1 - \sqrt{F_{max}}$$

Így:

$$T_{MK} = -\frac{1}{\lambda} \cdot \ln\left(1 - \sqrt{F_{max}}\right) = MTBF \cdot \ln \frac{1}{1 - \sqrt{F_{max}}}$$

Például ha MTBF = 1 [év] és F_{max} = 1 [%], akkor
T_{MK} = 0,104 [év] azaz kb. 1 hónap

Összehasonlításul határozzuk meg az előző példa eredményeinek felhasználásával a redundancia-mentes esettel szemben jelentkező előnyt.

7-6. példa:

Mekkora lenne az előző rendszer megbízhatósága redundanciamentes esetben, ha a fenti ideig (kb. egy hónapig) működtetnénk felügyelet nélkül?

Megoldás:

Az előbbi példa adataival számolva:

$$R(t) = e^{-\lambda \cdot T_{MK}} \approx 1 - \lambda \cdot T_{MK} = 1 - \frac{T_{MK}}{MTBF} = 89[\%]$$

vagyis a rendszer megbízhatóságát 89%-ról 99%-ra növeli a redundáns megoldás, azaz a kockázat a tartalékolt rendszerben 11%-ról 1%-ra csökken. Ezután felmerül természetesen a gazdaságosság kérdése, össze kell vetni a redundancia miatti költségnövekedést a több hiba miatt keletkező kiesések költségeivel.

A párhuzamos rendszerek meghibásodási tényezőjének alakulására vonatkozóan megállapítható, hogy ha csupa nem öregedő elemből építünk fel redundáns rendszert, annak meghibásodási tényezője mindenképpen időfüggő lesz, tehát a redundáns rendszerek minden esetben öregedő jellegűek (lásd a 7-19. ábra kapcsán a 7.3.6.1 fejezetben mondottakat).

Párhuzamos rendszert önmagában csak igen kivételes esetben lehet létrehozni. A párhuzamos tartalékolású rendszerek gyakorlati megvalósításához általában szükség van olyan további egységre is, amelyik a meghibásodott egységet kiiktatja és a még működő operatív egységek közül a soron lévő üzemképes egységnek adja át a rendszer funkcióját. Olyan rendszer, amelyik csak párhuzamos operatív egységekből épül fel, közös egység(ek) nélkül, csak ritkán fordul elő (például alkatrész-szintű redundanciáknál), mivel a logikailag párhuzamosan kapcsolódó operatív egységek be- és kimenetét általában nem lehet egyszerűen áramkörileg párhuzamosan kapcsolni. Ezért is kell olyan **közös** egység, amelyik érzékeli, ha a funkcionáló egység meghibásodott és helyette egy másikra kell átkapcsolni. Ezen kívül lehetséges, hogy az operatív egységeket ellátó tápegység is közös, tehát a rendszernek több logikailag soros, közös eleme is lehet. Ezért párhuzamos struktúrával általában nagyobb rendszerek részrendszereiként találkozunk csak.

A közös egységet tartalmazó tartalékolt rendszereket általánosan értelmezve lehetnek:

- forró-tartalékoltak,
- csökkentett terheléssel működő tartalékolásúak (stand-by) rendszer és
- hideg-tartalékoltak.

A stand-by rendszerekben mindig csak egy egység funkcionál, a többi terheletlen, vagy csökkentett terhelésű és ezért a meghibásodási tényezője rendszerint sokkal kisebb, mint az üzemben lévőé. Sőt a tartalék egység lehet teljesen kikapcsolva is és ekkor meghibásodása esetleg teljesen kizárható. Ezt az utóbbi esetet hideg tartalékolásnak nevezik. Az egységek füg-

gősége miatt sem a csökkentett terhelésű (stand-by), sem a hidegtartalékolt rendszer nem kanonikus, modellezésüket a 7.3.5. fejezetben tárgyaljuk.

Összefoglalva: **A kanonikus modellen alapuló számítási módszerek csak a forrótartalékolású rendszer megbízhatósági analízisére adnak lehetőséget,** mivel csak a „forró" tartalékolás esetén független valamennyi működőképes operatív egység meghibásodásának valószínűsége attól, hogy melyik egység látja el a rendszer funkcióját és melyik a tartalék.

7.3.2.4. Összetett kanonikus struktúrák

A rendszer kanonikus jellege megmarad, ha csak soros és párhuzamos részekből (részrendszerekből) soros és/vagy párhuzamos struktúrával épül fel. Egy tartalékolt operatív részrendszert és egy soros közös részrendszert tartalmazó, soros struktúrájú, nem javított esetre általában az eredő megbízhatóság:

$$R_{\text{eredő}}(t) = R_p(t) \cdot R_s(t)$$

ahol

- $R_p(t)$ – az operatív egységekből felépülő párhuzamos részrendszer megbízhatósága,
- $R_s(t)$ – pedig a közös (soros) egység(ek) eredő megbízhatósága.

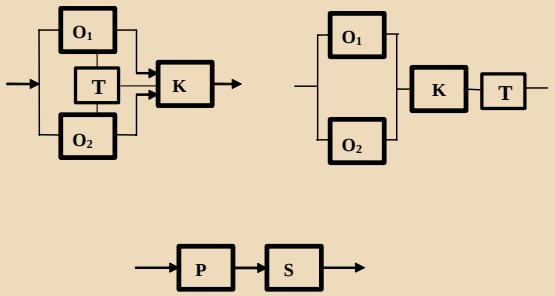
A legegyszerűbb ilyen összetett rendszert mutatja be az alábbi példa.

7-7. példa:

Két operatív egységből és közös egységekből (például tápegység, átkapcsoló) felépített kanonikus rendszer megbízhatósági modelljét mutatja a 7-5. ábra. Példánkban a párhuzamos egységek bemenetei áramkörileg közösíthetők, a kimeneteket azonban nem lehet egyszerűen összekötni, oda egy kapcsoló funkciójú soros egységre van szükség, valamint a rendszerhez tartozik egy közös tápegység is. Itt O_1 és O_2 a két operatív egység, P az előbbiekből felépülő párhuzamos részrendszer, S a soros részrendszer, amelyet a K kapcsoló és a T tápegység alkot.

$$R_{\text{eredő}}(t) = R_P(t) \cdot R_S(t)$$

$$R_S(t) = e^{-\lambda_S \cdot t} \qquad \text{ahol} \quad \lambda_S = \lambda_K + \lambda_T$$



7-5. ábra: Két operatív egységes rendszer két közös egységgel

$$R_P(t) = R_1(t) + R_2(t) - R_1(t) \cdot R_2(t)$$

$$R_1(t) = e^{-\lambda_1 \cdot t} \quad \text{és} \quad R_2(t) = e^{-\lambda_2 \cdot t}$$

Az S index a soros (közös) egységre, az 1, illetve 2 index a két operatív egységre, K a kapcsolóra, T a tápegységre vonatkozik. Ezzel

$$R_{\text{eredő}}(t) = e^{-(\lambda_1+\lambda_S)\cdot t} + e^{-(\lambda_2+\lambda_S)\cdot t} - e^{-(\lambda_1+\lambda_2+\lambda_S)\cdot t}$$

Legyen a két operatív egység egyforma erősítő, megbízhatóságuk: R_0, a kapcsoló megbízhatósága R_k és az egyszerűség kedvéért az időben állandó mindegyik, a tápegységet most figyelmen kívül hagyjuk.

a) eset: lemondunk a redundáns megoldásról: $R_a \equiv R_0$

b) eset: találunk egy ideális (mindig hibamentes) kapcsolót: ($R_k=1$)

$$R_b(t) = 1 - (1 - R_0)^2 = 2R_0 - R_0^2$$

Ez tényleg jobb lenne, mivel $R_b > R_0$, de ilyen sajnos nem létezik.

c) eset: a reális kapcsolós megoldást választjuk:

$$R_c = R_k \cdot (2R_0 - R_0^2)$$

Ha a kapcsoló csak ugyanolyan megbízható, mint az erősítők: $R_k = R_0$, akkor

$$R_c = 2R_0^2 - R_0^3 \le R_0$$

ez tehát biztosan nem jobb, mint az egyetlen erősítős redundancia mentes változat.

Indokolt kérdés: mennyi lehet legrosszabb esetben a kapcsoló megbízhatósága, ha a redundanciától javulást várunk? A követelményből, azaz $R_c > R_0$-ból:

$$R_k > \frac{1}{(2 - R_0)} > R_0$$

Látható, hogy ha a két erősítő nagy megbízhatóságú, akkor a kapcsolónak is igen jónak kell lennie, mivel egy rossz kapcsoló elrontaná a rendszert.

✸

7.3.3. Javított kanonikus struktúrák

Független elemű rendszerek esetében (ha az egyes elemek meghibásodási és a javítási folyamatai nem függenek egymástól), az egységek megbízhatósága (hibamentes működésük valószínűsége) helyett az **üzemképesség**gel kell számolni, vagyis az **r(t)** függvény helyére a **d(t)** függvény kerül. De mint korábban láttuk, az állandó értékű készenléti tényező igen jól közelíti az üzemképességet, így az időfüggvény helyett gyakran a konstans készenléti tényezőkkel is számolhatunk:
A soros (rész)rendszer készenléti tényezője:

$$K_s = \prod K_k \qquad (7\text{-}42)$$

a párhuzamos (rész)rendszerre pedig írható:

$$K_p = 1 - \prod (1 - K_k) \qquad (7\text{-}43)$$

ahol $\mathbf{K_k}$ az operatív egységek közül a k-adik készenléti tényezője.

7.3.4. Egyforma elemekből felépített kanonikus struktúrák

A kanonikus struktúrájú (rész)rendszerek egyik megvalósítása, amikor a rendszert **N** darab **egyforma**, a meghibásodási folyamatában egymástól független operatív egység alkotja. Például a stand by rendszer operatív részét alkotó egységek gyakran egyformák. A továbbiakban az összefüggéseket a javítás nélküli rendszerekre írtuk fel. A függetlenül javított esetben azonos formájú összefüggések adódnak, mindössze az **R(t)** függvények helyére a megfelelő **d(t)** függvényeket kell írni. Lehetséges az időben állandó készenléti tényezővel is számolni, az összefüggés erre vonatkozóan is hasonló.

Az egységek egyformák, tehát:

$$R_1(t) = R_2(t) = R_3(t) = \ldots = R_N(t) = R(t) \qquad (7\text{-}44)$$

Ez esetben annak valószínűsége, hogy az **N**-ből éppen **h** egység hibás (**N ≥ h** feltételezéssel), a **Bernoulli**-képlettel számítható:

$$P_{N,H}(t) = \binom{N}{h} \cdot \left[1 - R(t)\right]^{h} \cdot \left[R(t)\right]^{N-h} \qquad (7\text{-}45)$$

ahol

$$\binom{N}{h} = \frac{N!}{(N-h)! \cdot h!} \qquad (7\text{-}46)$$

Legyen a hibahatár úgy értelmezve, hogy a (rész)rendszer üzemképes, ha $h < M$, azaz üzemképtelen, ha $h \geq M$. Ekkor a (rész)rendszer üzemképességére írható:

$$R_{N,M}(t) = \sum_{i=0}^{M-1} P_{N,i}(t) \qquad (7\text{-}47)$$

Az ilyen struktúrák speciális esetei az alábbiak:

- az **N** egyforma elemből felépített **soros** rendszer, ekkor **M=1**
- az **N** egyforma elemből felépített **párhuzamos** rendszer, ekkor **M=N**
- az **N** egyforma elemből felépített **majoritásos** (többségi szavazati elven alapuló) rendszer, ekkor:

$$M = \frac{N+1}{2} \qquad (7\text{-}48)$$

- ahol **N** páratlan szám, értéke a gyakorlatban rendszerint 3, vagy 5, azaz **M = 2**, vagy 3. (Elvileg **N** bármekkora egynél nagyobb páratlan szám lehet.)

Az **N** elemű majoritásos rendszer operatív részére érvényes összefüggés:

$$R_{\text{majoritás}}(t) = \sum_{i=0}^{\frac{N-1}{2}} P_{N,i}(t) \qquad (7\text{-}49)$$

A teljes rendszer megbízhatóságának meghatározásakor figyelembe kell venni a szavazást és döntést végző **majoritás-logika** megbízhatóságát is. Mivel ez utóbbi egység strukturálisan sorosan kapcsolódik az egymással logikailag párhuzamosan kapcsolódó operatív egységekkel, a rendszer eredő megbízhatósága a szavazó **logikai egység** megbízhatóságának és a az **operatív** rész **(majoritásos alapon számított)** megbízhatóságának a szorzata:

$$R_{rendszer}(t) = R_{LE}(t) \cdot R_{majoritás}(t) \qquad (7\text{-}50)$$

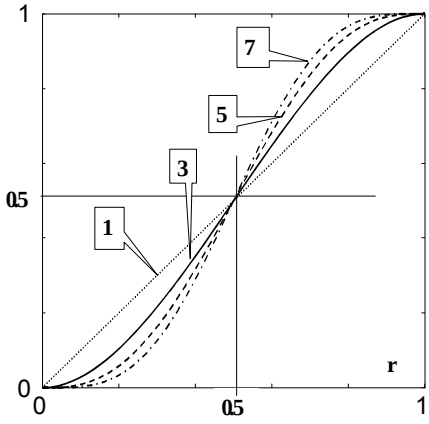
Hasonló összefüggéssel lehet az üzemkésséget is számítani.

$$K_{rendszer} = K_{LE} \cdot K_{majoritás} \qquad (7\text{-}51)$$

A 7-6. ábra a 3, az 5 és a 7 egységes majoritásos (rész)rendszer eredő megbízhatóság függvényét és a redundancia-mentes esetre (azaz egyetlen egységre) vonatkozó függvényt mutatja be az egység megbízhatósága (**R**) függvényében. Az ábrán a jelzőszámok az egységek számát (**N**) jelentik.

A majoritásos rendszer csak **R>0,5** esetben növeli a megbízhatóságot. Az ábrából látható, hogy ha **R<0,5** a rendszer megbízhatósága kisebb az egy egységénél.

$$R_{majoritás}(t) > R(t) \quad \text{ha} \quad R(t) > 0,5$$



7-6. ábra: Majoritásos (rész)rendszerek megbízhatóság függvénye

7-8. példa:

A 7-7. ábra egy háromegységes (N=3) majoritásos (rész)rendszer időfüggvényét mutatja:

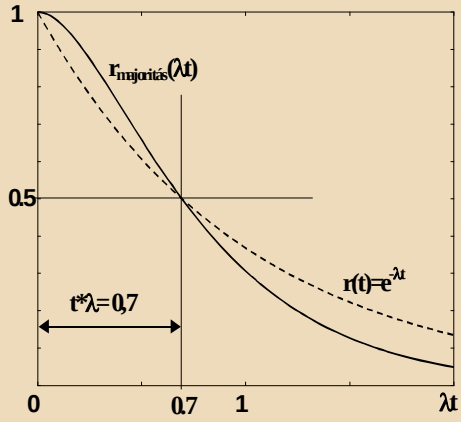
$$R_{\text{majoritás}}(t) = 3 \cdot e^{-2\lambda t} - 2 \cdot e^{-3\lambda t}$$

és a redundanciamentes (N=1) megoldás időfüggvénye $R(t) = e^{-\lambda t}$ látható: (A fenti képlet igazolása korábban már szerepelt.)

Az **r(t)=0,5**-höz tartozó t^* időpont: $t^* = \dfrac{0,7}{\lambda}$

mivel $0,5 = e^{-\lambda t^*}$, amiből $\ln 2 = \lambda \cdot t^*$

tehát $r_{\text{majoritás}}(t) > r(t)$ ha $t < t^*$



7-7. ábra: Háromegységes majoritásos (rész)rendszer és a redundanciamentes változat megbízhatóság-idő függvénye

A teljes rendszer megbízhatóságának meghatározásakor figyelembe kell venni a szavazást és döntést végző majoritás-logika megbízhatóságát is. Mivel ez utóbbi egység strukturálisan sorosan kapcsolódik az egymással logikailag párhuzamosan kapcsolódó operatív egységekkel, a rendszer eredő megbízhatósága a szavazó logikai egység megbízhatóságának és az operatív rész (majoritásos alapon számított) megbízhatóságának szorzata:

$$R_{\text{rendszer}}(t) = R_{\text{LE}}(t) \cdot R_{\text{maj}}(t) \qquad (7\text{-}52)$$

7-9. példa

A háromegységes majoritásos rendszer struktúráját a következő szemlélteti. Itt $\mathbf{O_1}$, $\mathbf{O_2}$ és $\mathbf{O_3}$ a három operatív egység, **LE** pedig a szavazást végző majoritás-logika egység.

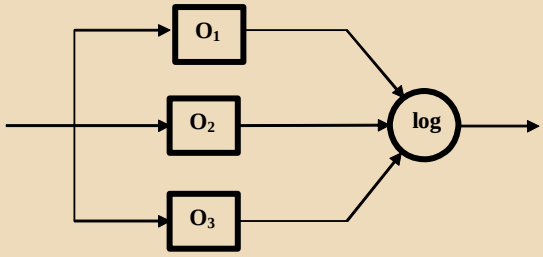
Az operatív rész megbízhatósága:

$$R_{\text{majoritás}}(t) = P_{3,0}(t) + P_{3,1}(t) = \binom{3}{0} \cdot R^3(t) + \binom{3}{1} \cdot R^2(t) \cdot [1 - R(t)]$$

vagyis

$$R_{\text{majoritás}}(t) = 3 \cdot R^2(t) - 2 \cdot R^3(t) = 3 \cdot e^{-2\lambda t} - 2 \cdot e^{-3\lambda t}$$

ahol λ az operatív egység meghibásodási tényezője.



7-8. ábra: Majoritásos rendszer struktúrája

Az első meghibásodásig várható működési idő kevesebb, mint ami egy redundancia-mentes esetre (egyetlen egységre) adódik, még akkor is, ha a logikai egység ideálisnak tekinthető.

$$T_{F,\text{majoritás}}(t) = \frac{3}{2 \cdot \lambda} - \frac{2}{3 \cdot \lambda} = \frac{5}{6 \cdot \lambda} < \frac{1}{\lambda}$$

Persze a logikai egység is meghibásodhat, jelölje λ' a logika meghibásodási tényezőjét. Ezzel a teljes rendszer megbízhatóságának időfüggvénye:

$$R_{\text{rendszer}}(t) = 3 \cdot e^{-(2\lambda+\lambda')\cdot t} - 2 \cdot e^{-(3\lambda+\lambda')\cdot t}$$

Tehát a működési idő tovább csökken (bár a valóságban nem számottevő mértékben, a gyakorlatban elfogadható közelítés: $\lambda' \approx 0$, hisz $\lambda' \ll \lambda$).

✸

7-10. példa:

Ötegységes majoritásos részrendszer megbízhatóság-idő függvénye:

$$R_{maj}(t) = P_{5,0}(t) + P_{5,1}(t) + P_{5,2}(t) =$$

$$\binom{5}{0} \cdot R^5(t) + \binom{5}{1} \cdot R^4(t) \cdot [1 - R(t)] + \binom{5}{2} \cdot R^3(t) \cdot [1 - R(t)]^2 =$$

$$21 \cdot R^5(t) - 42 \cdot R^4(t) + 21 \cdot R^3(t)$$

Ha $R(t) = e^{-\lambda \cdot t}$, akkor

$$T_{Fmaj} = \frac{21}{5 \cdot \lambda} - \frac{42}{4 \cdot \lambda} + \frac{21}{3 \cdot \lambda} = \frac{42}{60 \cdot \lambda}$$

✸

7-11. példa:

Hétegységes majoritásos részrendszer megbízhatóság-idő függvénye:

$$R_{maj}(t) = P_{7,0}(t) + P_{7,1}(t) + P_{7,2}(t) + P_{7,3}(t) =$$

$$\binom{7}{0} \cdot R^7(t) + \binom{7}{1} \cdot R^6(t) \cdot [1 - R(t)] + \binom{7}{2} \cdot R^5(t) \cdot [1 - R(t)]^2 +$$

$$+ \binom{7}{3} \cdot R^4(t) \cdot [1 - R(t)]^3 =$$

$$35 \cdot R^4(t) - 84 \cdot R^5(t) + 70 \cdot R^6(t) - 20 \cdot R^7(t)$$

✸

A tartalékolt párhuzamos egységek és a majoritásos rendszer operatív egységei nem mindig egyformák. Eltérő hardver és szoftver alkalmazása rendszerint növeli a megbízhatóságot (és persze a számítási munkát is). Viszont egyforma egységekkel felépített struktúrájú részrendszerek más megoldásokban is előfordulnak. Erre példa az alábbi.

7-12. példa

Egy adott 16 bites memória egység redundáns megvalósításban 6 checkbittel kiegészül. Ezáltal egy hibajavító mechanizmus az egy bit hibát önműködően kijavítani képes, két bit hiba esetén hibajelzést ad és automatikusan leállítja a rendszert. Kettőnél több hiba esetén hibásan tovább működik és rossz eredményeket szolgáltat. Legyen az egy bithez tartozó meghibásodási tényező: λ.

Mekkora a megbízhatóság, azaz mi a valószínűsége annak, hogy az egység hibátlanul működik (kettőnél kevesebb bit hibás): $R(t) = ?$

$$R(t) = P_{22,0}(t) + P_{22,1}(t) =$$

$$\binom{22}{0} \cdot R^{22}(t) + \binom{22}{1} \cdot R^{21}(t) \cdot \left[1 - R(t)\right] = 22 \cdot R^{21}(t) - 21 \cdot R^{22}(t)$$

vagy ha figyelembe vesszük, hogy $R(t) = e^{-\lambda \cdot t}$, ezért

$$R(t) = 22 \cdot e^{-21 \cdot \lambda \cdot t} - 21 \cdot e^{-22 \cdot \lambda \cdot t}$$

Innen az ehhez az állapothoz tartozó jó működési idő:

$$T = \frac{43}{462 \cdot \lambda}$$

A redundáns struktúra miatti javulás nem sok, ha csak a jó működési idő szempontjából értékeljük, hiszen redundancia nélkül, 16 operatív bittel számolva: $T' = \frac{1}{16 \cdot \lambda}$, innen $\frac{T}{T'} = 1,49$, tehát az időtartam 50%-nál is kevesebbet javul. (Ráadásul itt még nem vettük figyelembe azoknak az egységeknek a megbízhatatlanságát, amelyek a hibajavítást és a hibajelzést végzik. Amennyiben ezeket az egységeket nem tekintjük ideálisnak – hiszen a valóságban ezek is meghibásodhatnak – még kedvezőtlenebb a helyzet).

A redundáns struktúra révén elért látszólagosan csekély javulás, azonban **csak a várható jó működési időre vonatkozik.** Igen nagy megbízhatóságú rendszer jön létre, ha rövid időközönként karbantartó hibaelhárítást végeznek és az esetlegesen létrejött, de a rendszer működésében hibát nem okozó, egy bitnél nem több hibát elhárítják.

A megbízhatóság minimális értéke T_{MK} periodikus karbantartási idő esetén, ha $\lambda \cdot T_{MK} \ll 1$, az e^x függvény sorának első három tagjával közelítve adódik:

$$R(T_{MK}) \approx 22 \cdot \left[1 - 21 \cdot \lambda \cdot T_{MK} + \frac{(21 \cdot \lambda \cdot T_{MK})^2}{2!}\right] -$$

$$-21 \cdot \left[1 - 22 \cdot \lambda \cdot T_{MK} + \frac{(22 \cdot \lambda \cdot T_{MK})^2}{2!}\right]$$

vagyis $$R(T_{MK}) \approx 1 - 231 \cdot (\lambda \cdot T_{MK})^2$$

Fontos állapota a rendszernek, amikor a hiba: 0, vagy 1, vagy 2 bit. Ha kettőnél nem több hibás, akkor a rendszer vagy jól működik, vagy egyáltalán nem működik, azaz nem működik hibásan. Ez az állapot a felhasználó részére kedvezőbb annál, mint egy hibás továbbműködés. Jelölje ennek az állapotnak a valószínűségét P_2.

$$P_2(t) = P_{22,0}(t) + P_{22,1}(t) + P_{22,2}(t) =$$

$$= R(t) + 231 \cdot e^{-20 \cdot \lambda \cdot t} \cdot \left(1 - e^{-\lambda \cdot t}\right)^2$$

az ehhez tartozó működési idő:

$$T'' = \frac{231}{20 \cdot \lambda} + \frac{440}{21 \cdot \lambda} + \frac{210}{22 \cdot \lambda}$$

és innen $$\frac{T''}{T} \approx 37$$

✸

7.3.5. Általános struktúrák

A bonyolultabb rendszereket nem lehet a kanonikus struktúrákkal modellezni. A rendszer nem kanonikus,

a) ha nem soros/párhuzamos struktúrájú részek soros/párhuzamos kombinációja
b) ha kettőnél több állapottal kell a rendszert jellemezni
c) ha a rendszer elemeit kettőnél több állapottal lehet csak jól jellemezni

d) ha az elemek meghibásodása nem független egymástól
e) ha a javítás eseménykövető és nem kizárólag az üzemképtelenséget követő teljes felújítás.

A számítási modellek köre több irányban is bővíthető. A továbbiakban két módszert ismertetünk, amelyek közül megoldást adhat:

- a teljes valószínűség tétele – főleg az *a), b)* és *c)* esetben,
- az állapottér modell – főleg a *d)* és *e)* esetben.

ad *a)*
Előfordul, hogy a rendszer egyes részeinek működésére csak adott körülmények között van szükség, adott meghibásodások esetén a funkcionális struktúra megváltozik és ez soros/párhuzamos modellel már nem írható le.

ad *b)*
A rendszer hibás állapotai között különbséget kell tennünk, ha azokat nem egyformán javítják (javíthatók), ha nem teljes üzemképtelenséget okoznak, csak a rendszer egyes funkcióinak vagy a teljesítő képességének korlátozását eredményezik.

ad *c)*
Nem célszerű valamennyi alkatrészre csak egyféle rossz állapotot értelmezni, ha a rendszer állapotától függ az, hogy az adott típusú hiba milyen hatást okoz.

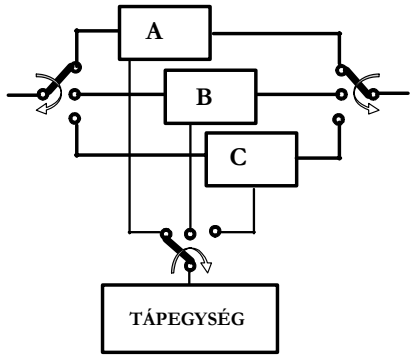
ad *d)*
A tartalékolt egységek meghibásodási folyamatát (meghibásodási tényezőjét) gyakran befolyásolja más egységek állapota, ilyen a hideg és a csökkentett terhelésű tartalék, vagy az üzemi terhelések eloszlásának megváltozása egyidejűleg működő egységek esetén.

ad *e)*
A javítási stratégia sokféle lehet. Nemcsak üzemképtelenség esetén és nem minden hibánál egyenlő intenzitással és egyforma végcéllal (teljes felújítás, vagy csak a hibák számának csökkentése) javítanak.

7.3.5.1. Hidegtartalék

Azt a redundáns, párhuzamos tartalékolású (rész)rendszert, amelyben mindig csak egyetlen egység működik és a tartalékban lévő többi nemcsak terheletlen, de ki is van kapcsolva és ebben az állapotban (a modell közelítése szerint) teljes biztonsággal kizárható a meghibásodása, hidegtartaléko-

lásnak nevezik. Ez a rendszer azért nem kanonikus, mivel **az egységek meghibásodási folyamata függ más egységek állapotától.**



7-9. ábra: Háromegységes hidegtartalékolt rendszer

A 7-9. ábra egy három egységes hidegtartalékolt rendszert mutat be, ahol kezdetben az **A** egység működik, annak meghibásodásakor a **B**, majd a **C** veszi át a funkciót. Az átkapcsolók nemcsak az operatív egységek be- és kimenetét, de a tápellátást is váltják, a kapcsolók meghibásodáskor késedelem nélkül egyszerre kapcsolnak. Kézenfekvő, hogy ebben az esetben a rendszer üzemképessége a három egység jó működési idejének összege:

$$T_{FH} = \frac{1}{\lambda_A} + \frac{1}{\lambda_B} + \frac{1}{\lambda_C} \qquad (7\text{-}53)$$

Ha pedig az egységek egyformák: $\lambda_A = \lambda_B = \lambda_C = \lambda$, akkor $T_{FH} = \frac{3}{\lambda}$

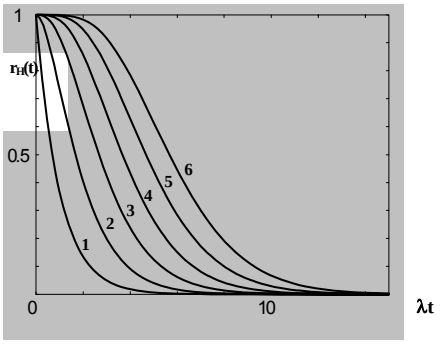
N egyforma egységre:

$$T_{FH} = \frac{N}{\lambda} \qquad (7\text{-}54)$$

A megbízhatóság időfüggvénye Poisson-eloszlást mutat. Annak valószínűsége, hogy **t** idő alatt egyforma hidegtartalékolású egységből **h**-nál nem több hibásodik meg:

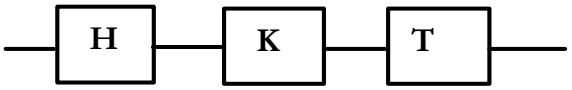
$$R_h(t) = e^{-\lambda \cdot t} \cdot \sum_{k=0}^{h} \frac{(\lambda \cdot t)^k}{k!} \qquad (7\text{-}55)$$

A 7-10. ábra a λt függvényében mutatja be ezt az összefüggést. Az „1” indexű görbe a tartalék nélküli: $R(t) = e^{-\lambda \cdot t}$, a „2” indexű görbe az egy hidegtartalékot tartalmazó (tehát összesen kétegységű) eset, a „3” indexű a háromegységes és így tovább.



7-10. ábra: Hidegtartalékolt (rész)rendszerek megbízhatóság-idő függvénye

Az ilyen rendszerek megbízhatósága a 7-11. ábra alapján jellemezhető, ahol H a hidegtartalékolt részrendszert, K a kapcsolókat, T a tápegységet jelenti.



7-11. ábra: Hidegtartalékolt rendszer

7-13. példa

Egy négyegységes hidegtartalékolt részrendszerben az első egység meghibásodásakor üzembe lép a második stb. A részrendszer addig üzemképes, amíg négynél kevesebb meghibásodás van. Ha az egységek egyformák, a meghibásodási tényezőjük λ.

$$T_{FH} = \frac{4}{\lambda} \quad \text{és}$$

$$R_H(t) = e^{-\lambda \cdot t}\left[1 + \lambda \cdot t + \frac{(\lambda \cdot t)^2}{2} + \frac{(\lambda \cdot t)^3}{6} + \frac{(\lambda \cdot t)^4}{24}\right]$$

✸

7.3.5.2. Kvázi redundanciák

Szigorúan értelmezve: a soros struktúrájú rendszer bármelyik elemének meghibásodása a rendszer működésképtelenségét eredményezi. Ez a modell valójában egyszerűsítő közelítése a valóságnak, mivel az ilyen rendszerek általában nem teljesen redundancia-mentesek: a soros struktúrájú elrendezések gyakran tartalmaznak redundanciát. Az alkatrészek specifikáció szerinti hibakritériuma rendszerint szigorúbb, mint az alkalmazásból adódó érték, a készülék működőképes maradhat, ha egyes elemeknél a paraméterek kilépnek a specifikált tűrés tartományból. A funkcionálisan párhuzamos redundanciát alkotó elemek viszont gyakran nem valamennyi előforduló hiba esetén ténylegesen redundánsak, adott hibánál sorossá válnak megbízhatósági szempontból.

Egyrészt tehát egyes redundancia-mentesként kezelt rendszerekben **rejtett redundancia** van, másrészt egyes tartalékolt struktúrák csak **kvázi redundáns**ak. A megbízhatósági számítások és a gyakorlati tapasztalatok között bizonyos ellentmondást jelenthet, ha ezeket a rejtett és kvázi redundanciákat figyelmen kívül hagyjuk a számítások során.

A meghibásodásokat ebből a szempontból két csoportra célszerű osztani: okozhatnak passzív és aktív hibát.

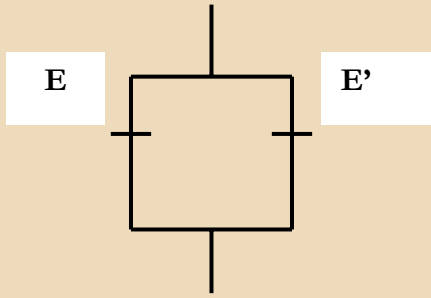
A **passzív hiba „kiesés”** jellegű, tehát mintegy az adott elem hiányát jelenti. Az ezzel a fajta hibával meghibásodott egység a rendszer szempontjából nem létezik. Ilyen például, ha sínre kapcsolódó egységek közül az egyiknek szakadás jelleggel szűnik meg a kapcsolata sínnel. Ez esetben a rendszer üzemképes maradhat, ha az adott egységből még van a sínre csatlakozó tartalék.

Aktív hiba esetén az egység hibája a rendszer működésében zavart okoz. Ebben az esetben hiába lenne az adott egységből tartalék, a rendszer minden képen működésképtelenné válik, tehát a párhuzamos tartalékot képező elem megbízhatóság szempontjából sorossá válik. Ilyen például, ha a sínre kapcsolódó egységek közül az egyik **zárlat** jelleggel hibásodik meg. A kétféle hiba **egység szinten** általában leszakadás (open tipusú hiba) és rövidzárlat (short tipusú hiba) formájában jelentkezik (például közös sínre kapcsolódó redundáns párhuzamos egységeknél). **Alkatrész szinten** tartalékolás nélküli esetben legfeljebb a másodlagos meghibásodások szempontjából van értelme a kétféle hibát megkülönböztetni (például a rövidzárlat további meghibásodást okoz, a szakadás nem). Tartalékolt (redundáns) alkatrészekkel megvalósított áramkörben a kapcsolástól függően a szakadás és zárlat egyaránt lehet passzív és aktív hiba is.

A problémakör illusztrálására szolgálnak az alábbi példák. Egy lehetséges analízist a 7.3.5.3 fejezet tartalmaz.

7-14. példa:

Egy áramkörben a kapcsolót a megbízhatóság növelésére megkettőzik. A két kapcsolót lehet sorosan is, párhuzamosan is kötni. Ha párhuzamosan vannak kötve, a zárlat (állandóan bekapcsolva marad) aktív hibaként jelentkezik, a szakadás (nem tud bekapcsolni) viszont passzív hiba. Ha a két kapcsolót sorosan kötik, pontosan fordított a helyzet.

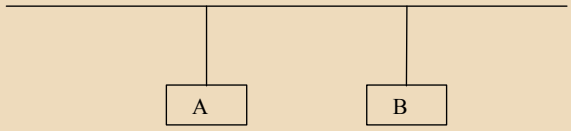


7-12. ábra: Megkettőzött munkaérintkező

✸

7-15. példa:

Közös tápvezetékre kapcsolódó funkcionálisan párhuzamos egységek a gyakorlatban csak kvázi redundánsak, mivel ki kellene zárnunk a tápvonalnak általuk okozható túlterhelését, zárlatát. Utóbbi esetben soros struktúrát alkotnak megbízhatóság szempontjából akkor is, ha funkcionálisan párhuzamosak lennének (7-13. ábra.



7-13. ábra: Sín struktúra

✸

7-16. példa:

Egy többféle szolgáltatást adó, soros rendszerben rejtett redundancia keletkezik, ha az tartalmaz olyan elemeket, egységeket, amelyeket a rendszer ritkán használ, amelyek működésére csak kis valószínűséggel van szükség. Az ilyen, ritkán használt elem kiesése (passzív jellegű hibája) csak akkor okozza a rendszer működésképtelenségét, ha éppen szükség lenne rá. Ilyen esetben a hibakritériumot vagy az alkatrész meghibásodási tényezőjét lehetne módosítani: az alkalmazásból adódó szükségesség mértékében arányosan csökkenteni. Ezzel a realitásokhoz jobban illeszkedő megbízhatósági adatot kapnánk, azonban az nem a készülék specifikáció szerinti jó állapotához, csak az adott alkalmazáshoz tartozó adat lenne.

Például ilyen egy villámvédelmet szolgáló túlfeszültség-levezető alkatrész, aminek „hiány" jellegű meghibásodása nem derül ki az első villámcsapásig. Ha a túlfeszültség levezető zárlatát ki lehetne zárni, akkor ezt az alkatrészt a számításokban teljesen figyelmen kívül hagyva reálisabb közelítést érnénk el, mint ha a teljes meghibásodási tényezőjével vennénk számításba.

✸

7-17. példa:

Kétegységes forrótartalékolt rendszer egységeinél értelmezhető passzív és aktív jellegű hiba. Az adott példa szerint egy adott egység aktív hibáját nem követheti passzív, illetve fordítva és rendszerhiba esetén van teljes felújítás.

$$\lambda = \lambda_A + \lambda_P$$

ahol λ_A az aktív,
λ_P a passzív jellegű hibához tartozó meghibásodási tényező.

$$\frac{\lambda_P}{\lambda} = \alpha < 1$$

A problémakörhöz tartozó számítás a későbbiek során ismertetésre kerülő eljárást igényli, (lásd a 7.3.6.3 fejezetet).

A számítás részletezése nélkül: $T_F = \frac{(1 + 2 \cdot \alpha)}{2 \cdot \lambda}$

✸

7-18. példa:

Az áramköri kártyák nagy részén a tápáramkör szűrésére több szűrőkondenzátort alkalmaznak. Egy-egy ilyen kondenzátor jelentős mértékű kapacitáscsökkenése, sőt teljes hiánya (szakadása) gyakran nem eredményez semmilyen hibát. Persze bármelyik kondenzátor zárlata működésképtelenné tenné az áramkört.
Legyen a kondenzátor meghibásodási tényezője:

$$\lambda_C = \lambda_Z + \lambda_{SZ}$$

ahol λ_Z – a zárlathoz (és az átvezető áram erős növekedéshez) -,
λ_{SZ} – a szakadáshoz (és a jelentős kapacitás csökkenéshez) tartozó érték.

A kártyán lévő **n** darab kondenzátor bármelyikének zárlata a kártya üzemképtelenségét okozza. Ennél kevesebb, **m<n** darab kiesése viszont még nem. Az ezekből adódó eredő meghibásodási tényező:

$$\lambda = n \cdot \lambda_Z + (n - m) \cdot \lambda_{SZ}$$

és ezzel $\lambda < n \cdot \lambda_C$

Az m/n arány csak közelítésekkel becsülhető.

✸

7.3.5.3. A teljes valószínűség tétel alkalmazása

A kanonikus módszerrel nem kezelhető struktúrák közül több analizálható a teljes valószínűség tétel segítségével. Ilyenek a kettőnél több állapottal leírható elemekből felépülő rendszerek és a soros-párhuzamos struktúrával nem modellezhetők. Utóbbiak két alaptípusa: a híd struktúra és azok a funkcionális modellek, amelyekben egy adott egység olymódon szerepel több helyen, hogy a megbízhatóság struktúrában nem vonható össze. Az alábbiak példákat mutatnak be az alaptípusokra.

Az alkalmazott jelölések:

Pr{A} annak a valószínűsége, hogy a vizsgált objektum az **A** állapotban van. (Például, hogy a rendszer üzemképtelenné vált.) Az **A** állapot függ

a $\mathbf{B_1}$, $\mathbf{B_2}$...$\mathbf{B_n}$ eseményektől. (Például, hogy a rendszert alkotó valamelyik adott elem zárlatos lett.)

Pr{A | $\mathbf{B_i}$} az A feltételes valószínűsége a $\mathbf{B_i}$ feltételre vonatkoztatva. (Például annak valószínűsége, hogy a rendszer üzemképtelen, ha az adott eleme zárlatos.)

A teljes valószínűség tétel szerint:

$$\Pr\{A\} = \sum_{i=1}^{n} \Pr\{A|B_i\} \cdot \Pr\{B_i\} \qquad (7\text{-}56)$$

ha $\mathbf{B_i}$ és $\mathbf{B_j}$ egymást kölcsönösen kizárják $\forall i \neq j$-re,
és $\mathbf{B_1}$, $\mathbf{B_2}$...$\mathbf{B_n}$ az adott elemre vonatkozóan a teljes eseményteret lefedik,

azaz $$\sum_{i=1}^{n} \Pr\{B_i\} = 1$$

(Például $\mathbf{B_1}$ = az elem jó, $\mathbf{B_2}$ = passzív hibája van, $\mathbf{B_3}$ = aktív hibája van és az elemnek e hármon kívül nem létezik több állapota.)

7-19. példa:

Egy jelfogó megbízhatóságának növelése érdekében két egyforma munkaérintkezőjét (É, É') párhuzamosan kapcsolva megkettőzik (7-12. ábra).

Párhuzamos kapcsolás esetén az elem passzív hibáját jelenti, ha az nem tud zárni és aktív hibáját, ha nem tud bontani (zárlatos lett). Soros kapcsolás esetén fordított a helyzet: aktív a hiba, ha nem tud zárni (szakadt lett) és passzív, ha nem tud bontani (zárlatos lett).

A megkettőzött érintkezőből álló „rendszer" működőképessége az A esemény. A két egyforma elem közül önkényesen kiválasztva az egyiket (É') annak három állapota alkotja a feltétel rendszert. (B_1' = az érintkező jó, B_2' = passzív hibája van, B_3' = aktív hibája van és e hármon kívül nincs több állapota.)

$\Pr\{A|B_1\} = \Pr\{B_1'\} \cdot \Pr\{B_2'\}$ (az egyik jó, a másik jó, vagy passzív hibás)

$\Pr\{A|B_2\} = \Pr\{B_1'\}$ (az egyik passzív hibás, a másik jó)

$\Pr\{A|B_3\} = 0$ (ha az egyik aktív hibás, akkor a rendszer nem lehet jó)

$$\Pr\{A\} = \Pr\{B_i\} \cdot \left[\Pr\{B_1^{'}\} + \Pr\{B_2^{'}\}\right] + \Pr\{B_i\} \cdot \Pr\{B_2^{'}\} + 0$$

A kétérintkezős rendszer megbízhatósága a redundancia-mentes (egyérintkezős) megoldás megbízhatóságára vonatkoztatva:

$$\frac{\Pr\{A\}}{\Pr\{B_1\}} = \Pr\{B_1\} + 2 \cdot \Pr\{B_2\} =$$
$$= 1 - \left[\Pr\{B_2\} + \Pr\{B_3\}\right] + 2 \cdot \Pr\{B_2\} =$$
$$= 1 + \Pr\{B_2\} - \Pr\{B_3\}$$

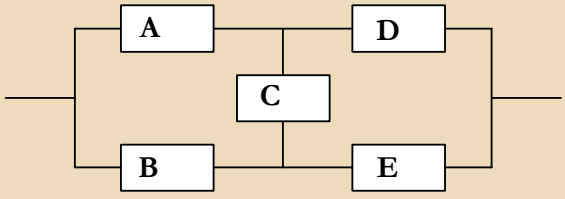
Tehát, ha **$\Pr\{B_2\} > \Pr\{B_3\}$**, akkor a redundáns megoldás eredményes. Ha nem, akkor kár volt a két érintkezőt párhuzamosan kapcsolni. Nyitott jelfogók, kisterhelésű kapcsolók esetében a megbízhatóságot növeli a párhuzamos kapcsolás, de védőgázas (reed) jelfogók, vagy diódával megvalósított kapcsolók esetében nem, mivel ott **$\Pr\{B_2\} < \Pr\{B_3\}$**. Így ilyenkor a soros kapcsolás növeli a megbízhatóságot, mert ekkor (a hasonló számítás mellőzésével):

$$\frac{\Pr\{A\}}{\Pr\{B_1\}} = 1 + \Pr\{B_3\} - \Pr\{B_2\}$$

✸

7-20. példa:

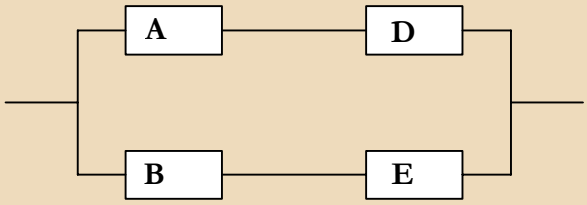
A **V** és a **W** pontokat összekötő távbeszélő hálózat kétirányú forgalomra alkalmas **A**, **B**, **C**, **D**, **E** szakaszokból redundánsan épül fel. A **C** hídág, a 7-14. ábra szerint.



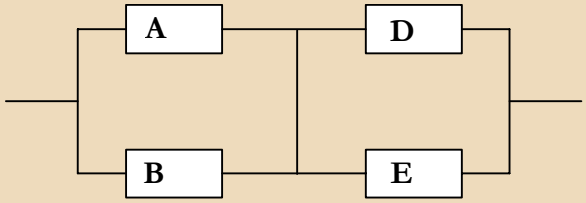
7-14. ábra: Híd modell-1.

A forgalomirányítás alapesete az **AD** útvonal. Meghibásodás esetén a **BE** párhuzamos út a másodlagos. Az **A** és **E**, vagy a **B** és **D** ágak egyidejű hibája esetén a **C** hídág segítségével bonyolódhat le a forgalom a még működőképes **B** és **D** vagy **A** és **E** ágakon.

Ha **C** ág nem működik, akkor a 7-15. ábra szerinti a struktúra, ha **C**-re is szükség van, akkor a 7-16. ábra szerinti.



7-15. ábra: Híd modell – 2.



7-16. ábra: Híd modell – 3.

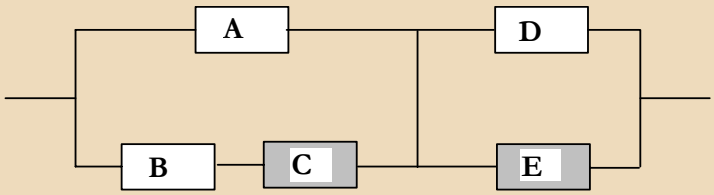
Itt $\mathbf{B_1 = C}$ nem üzemképes, $\mathbf{Pr\{B_1\} = 1 - R_C}$
$\mathbf{B_2 = C}$ üzemképes, $\mathbf{Pr\{B_2\} = R_C}$

$$R_{híd} = (1 - R_C) \cdot [R_A \cdot R_D + R_B \cdot R_E - R_A \cdot R_B \cdot R_D \cdot R_E] +$$
$$+R_C \cdot [(R_A + R_B - R_A \cdot R_B)(R_D + R_B - R_D \cdot R_E)]$$

✸

7-21. példa:

Ha a két – 7-17. ábra szerinti – **C** jelű egység azonos, a feltételes valószínűségek itt is az előző példa szerintiek: a **C** egység két állapotának megfelelően.



7-17. ábra: Hídmodell 4.

$$R_{eredő} = (1 - R_C) \cdot (R_A \cdot R_D) + R_C \cdot (R_A + R_B - R_A \cdot R_B) \cdot (R_D + R_E - R_D \cdot R_E)$$

✸

7-22. példa:

Közös sínre kapcsolódó két egyforma egységből álló redundáns részrendszer, ahol az egységek a fent leírt háromféle állapottal (kétféle hibával) jellemezhetők, javítás nincs.

Az egységek egyformák, állapotindexeik:

x=0 : jó állapot, ennek valószínűsége:	$\mathbf{P_0(t)}$
x=1 : passzív hiba van, ennek valószínűsége:	$\mathbf{P_1(t)}$
x=2 : aktív hiba van, ennek valószínűsége:	$\mathbf{P_2(t)}$
Az állapotvektor:	$\mathbf{X = [X_A, X_B]}$
A rendszer-függvény:	**Y(X)**

A rendszer állapotindexei:

Y=0 : üzemképes, ennek valószínűsége:	**r(t)**
Y=1 : működésképtelen, ennek valószínűsége:	**1 − r(t)**.

$$Y = 0, \quad \text{ha} \quad X = [0,0] \vee X = [0,1] \vee X = [1,0]$$

Ez alapján a rendszerre írható:

$$r(t) = [P_0(t)]^2 + 2 \cdot P_0(t) \cdot P_1(t)$$

7-23. példa:

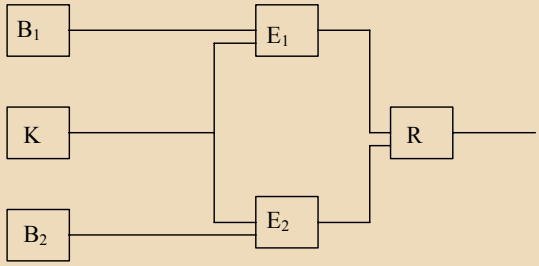
A repülőgép pilótája és másodpilótája rendelkezik a sisakjához szerelve egy-egy mikrofont és fejhallgatót tartalmazó ($\mathbf{B_1}$ és $\mathbf{B_2}$) egyforma egységgel, ezek az saját egyforma erősítőjükön ($\mathbf{E_1}$ és $\mathbf{E_2}$) kapcsolódnak a rádió adó-vevő készülékhez **(R).** A sisak-egységek meghibásodása esetén van egy közös kézibeszélő **(K)** is és ez bármelyik működőképes erősítőn ke-

resztül csatlakozhat a rádióhoz. (Ez egy olyan rendszer, amelyik azért nem kanonikus, mert az egyik egység a rendszer struktúrájában – megbízhatósági modelljében – két helyen szerepel). A rendszer vázlatát a 7-18. ábra mutatja.

Mekkora a rendszer **R(t)** megbízhatósága, ha az **E** erősítőké $\mathbf{R_E(t)}$, az **R** rádióé $\mathbf{R_R(t)}$, a **B** beszélő egységeké $\mathbf{R_B(t)}$. Legyen a feltételrendszer a közös egység jó és rossz állapota, az ezekhez tartozó valószínűség: $\mathbf{R_K(t)}$, illetve $\mathbf{1\text{-}R_K(t)}$. A hibakritérium pedig az, hogy egyik pilóta sem tud kommunikálni.

Így

$$R(t) = R_K(t) \cdot \left[2R_E(t) - R_E^2(t)\right] \cdot R_R(t) + \\ + \left[1 - R_K(t)\right] \cdot \left[2R_B(t) \cdot R_E(t) - R_B^2(t) \cdot R_E^2(t)\right] \cdot R_R(t)$$



7-18. ábra: Példa redundáns struktúrára

7.3.6. A Boole-modell alapján végzett vizsgálatok gyakorlati eljárásai

7.3.6.1. Hibafa elemzési módszer

1. A módszer elvi alapjai, a hibafa felállítása

A hibafa elemzés, **FTA** = **F**ault **T**ree **A**nalysis, igen áttekinthető formában teszi lehetővé a rendszer megbízhatósági szempontból történő elemzését. A Boole-féle megbízhatósági módszerek elterjedésével olyan grafikus ábrázolási módot fejlesztettek ki, mellyel a mérnöki szemlélet számára áttekinthető formában ábrázolják az elemek és a rendszer meghibásodásának kapcsolatát. Mivel ez a modell a Boole-féle megbízhatósági modell alapján áll, ezért az olyan rendszereknél, melyeknél többféle rendszerállapot előfordulhat, minden vizsgálandó eseményre (akadályozó- vagy veszélyes hiba, zárlat vagy szakadás stb.) külön hibafát kell meghatározni. Így ezt a

módszert a vasúti automatikáknál, de egyéb biztonsági területeken, atomerőművi-, katonai alkalmazásoknál is jól felhasználták. A fa struktúra révén ez a modell könnyen továbbfejleszthető, de előnye még, hogy a műszaki rendszerrel nem téveszthető össze – ami az egyszerű megbízhatósági helyettesítő képről nem mondható el egyértelműen.

A hibafa módszer kiindulópontja a nemkívánatos célesemény, a rendszer meghibásodása. Ehhez minden lehetséges okot meg kell határozni – amihez természetesen jól kell ismerni a vizsgálandó rendszer működését.

A hibafa módszer értékeléseként a következőket mondhatjuk:

- a hibafák felállításához a rendszerek működésének és a hibamechanizmusok alapos ismerete szükséges,
- a vizsgálat célja és a vizsgált események terjedelme között ésszerű kompromisszumot kell találni,
- terjedelmes rendszerek esetén a hibafák manuális felállítása igen munkaigényes,
- a biztonsági rendszerek vizsgálatakor általában több hibafát kell felállítani.

Fentiekből következik, hogy a hibafák felállítását lehetőleg annyira formalizálni kell, hogy azt számítógép segítségével lehessen végezni. Erre vonatkozóan már vannak konkrét megoldások, de általában bonyolult rendszerekre még nem.

2. Matematikai számítások

A hibafa felállítás után a következő lépés a megbízhatósági vizsgálatok számára alkalmas matematikai modell kiválasztása. Az **ÉS-** és **VAGY-tag**okra megfogalmazhatók a feltételek, amelyek aztán könnyen általánosíthatók.

VAGY-tag

Meghibásodás akkor következik be, ha vagy az egyik, vagy a másik tag meghibásodik. Eszerint ebben az esetben soros rendszerről van szó. Amiből következik, hogy:

$$F_{VAGY} = F_1(t) + F_2(t) - F_1(t) \cdot F_2(t) \qquad (7\text{-}57)$$

Egy **n** eseményből álló **VAGY tag** esetén a következő összefüggés adódik:

$$F_{VAGY} = 1 - \prod_{i=1}^{n}\left[1 - F_i(t)\right] \text{ vagy } R_{VAGY} = \prod_{i=1}^{n} R_i(t) \qquad (7\text{-}58)$$

ÉS-tag

Meghibásodás akkor lép fel, ha két elem esetén az E1 és E2 egyaránt meghibásodik. Vagyis ebben az esetben párhuzamos rendszerről van szó, amelyre a következő összefüggések adódnak:

$$F_{ÉS}(t) = F_1(t) \cdot F_2(t) \qquad (7\text{-}59)$$

Valamely **n** eseményből álló **ÉS tag**ra a következő összefüggéseket kapjuk:

$$R_{ÉS} = 1 - \prod_{i=1}^{n}\left[1 - R_i(t)\right] \text{ vagy } F_{ÉS} = \prod_{i=1}^{n} F_i(t) \qquad (7\text{-}60)$$

A logikai függvények meghibásodási rátára vonatkozó vizsgálata a következő eredményekhez vezet:

Ha az események meghibásodási rátája állandó, akkor a VAGY tagra is állandó meghibásodási ráta adódik, amely az egyes események meghibásodási rátáinak összegeként adódik. Ez az összegzési tétel időben változó meghibásodási ráták esetén is érvényes. Matematikailag megfogalmazva:

$$\lambda_{VAGY}(t) = \sum_{i=1}^{n} \lambda_i(t) \qquad (7\text{-}61)$$

Ha az események meghibásodási rátája állandó, akkor az **ÉS tag**ra az igénybevételi időtől függő meghibásodási ráta adódik a következőképpen:

$$\lambda_{ÉS}(t) = \frac{\sum_{i=1}^{n} \lambda_i(t) \cdot (\alpha_i - 1)}{\prod_{i=1}^{n} \alpha_i - 1} \qquad (7\text{-}62)$$

ahol

$$\alpha_i = \frac{1}{1 - e^{-\lambda_i \cdot t}} \qquad (7\text{-}63)$$

Az események azonos meghibásodási rátája esetén a következő összefüggést kapjuk:

$$\lambda = \frac{n \cdot \lambda}{\alpha^{n-1} + \alpha^{n-2} + \ldots + \alpha + 1} \tag{7-64}$$

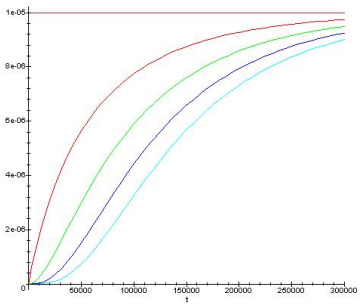
ahol

$$\alpha = \frac{1}{1 - e^{-\lambda \cdot t}} \tag{7-65}$$

A párhuzamos rendszerek meghibásodási tényezőjének alakulását mutatja a következő ábrán látható görbesereg (7-19. ábra). A vízszintes egyenes mutatja az egyetlen elem meghibásodási ráta értékét, az alatta sorakozó görbék pedig a λ alakulását az egyre növekvő fokszámú redundancia esetén mutatják (a görbék egymásután az n = 2, 3, 4 és 5 esetre vonatkoznak).

7.3.6.2. Hibahatás elemzés

A rendszerek vizsgálatának másik igen fontos módszere a hibahatás elemzés, az **FMEA** = **F**ailure **M**odes and **E**ffects **A**nalysis). Ez a módszer az egyes alkatrészek lehetséges meghibásodásainak és az ez által érintett további alkatrészek szisztematikus vizsgálatát jelenti, az üzemkészségre illetve a biztonságra gyakorolt hatásuk alapján. Ez utóbbi esetben az elnevezés is bővül és **FMECA**-ról beszélünk (= **F**ailure **M**odes, **E**ffects and **C**riticality **A**nalysis). A vizsgálatnak figyelembe kell venni a lehetséges hibafajtákat és hiba-okokat. A módszer segítségével meghatározhatók a potenciális veszélyeket (erről még részletesebben lesz szó a 8.1 fejezetben). Ezzel lehetővé válik a meghibásodások hatásának kiküszöböléséhez illetve e hatások és a meghibásodások valószínűségének csökkentéséhez szükséges intézkedések meghozatala, elemzése.



7-19. ábra: A párhuzamos rendszer meghibásodási tényezőjének alakulása

7.3.6.3. A két módszer értékelése

A két módszer alapján végzett vizsgálatokat áttekintve megállapítható, hogy kiindulási alap mindkettő esetében egy fa struktúrájú irányított gráf. Az előzőek szerint a hibafa elemzés a rendszer meghibásodásából, mint csúcseseményből indul ki és ehhez keresi meg szisztematikusan. hogy milyen alkatrész meghibásodások eredményezhetik ezt. Ilyen módon ezt egy top-down (deduktív) módszernek tekinthetjük.

Az FMEA/FMECA módszer az alkatrészek meghibásodásából és ebből határozza meg ennek rendszerre gyakorolt várható hatását, így ez ún. bottom-up (induktív) módszert jelent.

Az eljárás logikáját tekintve könnyen belátható, hogy a két módszer együttes alkalmazása jelenthet teljes megoldást. Az FMEA/FMECA szisztematikusan végigvizsgálja az alkatrészek lehetséges meghibásodásait, de nem vizsgálja az egyes meghibásodások kölcsönös egymásra hatásait. Ezt inkább az FTA teszi lehetővé. A rendszer meghibásodásból kiinduló vizsgálat viszont nem biztos, hogy valamennyi alkatrész-meghibásodáshoz eljut. A tapasztalat azt mutatja, hogy a két módszer egymást kölcsönösen kiegészíti, a két módszer együttes alkalmazása jelent megfelelő megoldást. A nagyobb rendszerek vizsgálatának megkönnyítésére mindkét probléma megoldására megfelelő számítógépes programok állnak rendelkezésre. A szoftver fejlesztők a két módszerre alkalmas programokat együtt fejlesztik, a szoftverpiacon is általában együtt kaphatók.

7.4. Az állapottér modell (az ún. Markov-féle modell)

7.4.1. A Boole-modell alkalmazásának értékelése

Az előző fejezetben láthattuk a Boole módszer számos előnyét, mint pl.:

- független az elosztástípustól
- logikailag jól áttekinthető
- egyszerűen ábrázolható
- komplex rendszerek számjellemzői egyszerűen meghatározhatók

Ugyanakkor korlátait is megismerhettük:

- olyan rendszerek analízisére nem alkalmasak, amelyek struktúrája nem kanonikus és/vagy
- kettőnél több állapottal jellemezhető egységeket tartalmaznak, illetve

- maga a rendszer csak kettőnél több állapottal modellezhető (különböző meghibásodási módok figyelembevétele nehézkesen volt csak lehetséges),
- monotónia tulajdonság nem mindig adott
- a rendszerkomponensek nem mindig függetlenek egymástól

Nem kanonikus a struktúra, ha nem lehet soros és párhuzamos részrendszerekre bontani, mert például ugyanaz az egység több részrendszerben is előfordul. Gyakori az is, hogy valamelyik egység meghibásodása esetén meg kell különböztetni a keletkező hibát aszerint, hogy a rendszerre milyen hatást gyakorol.

Amennyiben a kétféle hiba létezik és meghatározható külön is az előfordulásuk valószínűsége, akkor a rendszer modellezésekor három állapotot kell az adott egység(ek)re értelmezni:

jó – passzív hiba – aktív hiba.

A biztonságkritikus rendszerek vizsgálata esetén szintén több hibaállapot megkülönböztetése szükséges

jó – akadályozó hiba – veszélyes hiba.

Láthatóan a gyakorlati életben előforduló problémák gyakran kivezetnek a Boole módszer alkalmazhatósági köréből. Szükség van tehát olyan módszerre, ami lehetővé teszi a többállapotú rendszerek vizsgálatát is. A következőkben ilyen módszert fogunk megismerni.

7.4.2. Az állapottéren alapuló ún. Markov modell

A következőkben az állapottéren alapuló modelleknek egy elvileg szűk, azonban a gyakorlatban jelentős és széles körben alkalmazható változatát fogjuk tárgyalni.
Ez a modell a

(1) véges, diszkrét állapotterű,
(2) folytonos idejű,
(3) sztochasztikus

folyamatok speciális esete, a

(4) markovi (emlékezetmentes),
(5) (időben) homogén,
(6) ergodikus

folyamat.

Az **(1)…(6)** szerint kiemelt meghatározások jelentését a továbbiakban röviden ismertetjük. Az ezekből adódó korlátozások ellenére a rendszerek legfontosabb jellemzői meghatározhatók:

- karbantartott (javított) redundáns rendszerek egyes állapotaiban való tartózkodás valószínűségének stacioner eloszlása, így a
- rendszer készenléti tényezője is és
- az egyes állapotokban és állapotcsoportokban való tartózkodás várható időtartama, valamint (bizonyos korlátozásokkal)
- nem javított rendszerek esetében a rendszer működésképtelenségéig várható időtartam.

Egyébként a kevésbé leszűkített (nem ergodikus, inhomogén) modell lehetőséget adna általánosabb esetek analízisére. Bonyolultabb számításokkal több, itt nem tárgyalt tranziens időfüggvény is meghatározható.

A vizsgált rendszer megbízhatósági analízise **véletlen eseményekre** vonatkozik: a folyamat **sztohasztikus (3)** jellegű. A sztochasztikus folyamatok kezelése a valószínűség-számítás bizonyos kibővítését igényli, melynek során véletlen változók függvényeit kell elemezni. Sztochasztikus folyamat alatt értjük a $Z(t)$ rendszerállapot időbeli alakulását, melyet $\{Z(t), t \geq 0\}$ módon jelölünk. $Z(t)$ a rendszer állapota valamely $t \geq 0$ időpontban. A rendszer az idő folyamán felveheti a $Z_1(t), Z_2(t), ...Z_i(t), ...Z_n(t)$ állapotok valamelyikét, állapotindexeik pedig $x = 1, 2, ...i, ...n$. A rendszert ezek az **állapotok** és a közöttük – elvileg bármelyik időpillanatban bekövetkezhető – **átmenetek** jellemzik (meghibásodási és javítási események). Ilyenkor a sztochasztikus folyamat **folytonos idejű (2).**

A megbízhatóság elméletben a meghibásodáshoz, javításhoz, hibaelhárításhoz tartozó időtartamokat véletlen hosszúságúnak tekintjük, s ezen állapotok sztochasztikus folyamatát vizsgáljuk. A rendszer lehetséges állapotai egymástól elhatároltak, az **állapottér diszkrét (1),** az állapotok száma véges és a rendszer egyidejűleg csak az egyik állapotban lehet, vagyis az állapotok diszjunktak (egymást kölcsönösen kizáróak). Ezen kívül fontos, hogy a rendszer összes lehetséges állapotát figyelembe vegyük, vagyis hogy az állapottér teljes legyen. Emiatt az egyes állapotokhoz tartozó valószínűségek összege minden időpontban egységnyi:

$$\sum_{x=0}^{n} P_x(t) = 1 \qquad (7\text{-}66)$$

A gyakorlatban előforduló rendszerek jelentős része kielégítően modellezhető struktúrán alapuló modellekkel, azonban nem használhatók ezek a modellek, ha általánosabb javítási stratégiát alkalmaznak és/vagy ha a meghibásodási folyamatok befolyásolhatják egymást. Az állapottér modell tovább bővíti a lehetőségeket, módot ad állapotfüggő meghibásodási és javítási folyamatok kezelésére is. A módszer lényege a rendszer lehetséges **állapot**aira és az azokat megváltoztató **esemény**ekre (állapotváltozásokra) alapuló analízis.

Átmenetet okozó esemény kétféle lehet: valamelyik elem **meghibásodás**a, vagy valamilyen **javítás,** hibaelhárítás. Az átmenetek valószínűségét meghatározza az esemény gyakorisága és az a feltétel, hogy a rendszer az eseményt megelőző állapotban van. Amennyiben a változást nem befolyásolják a korábbi állapotok, csak a közvetlenül megelőző, akkor a folyamat **emlékezetmentes,** egylépéses **markovi** folyamatnak nevezik. Ezt feltételnek tekinthetjük, mivel adott esetben az állapotteret megfelelő állapotokkal kibővítve, az esetleges „korábbi" hatásokat is figyelembe lehet venni a gyakorlatban.

A Markov tulajdonság matematikailag megfogalmazva, a feltételes valószínűségek felhasználásával:

$$\Pr\left\{Z(t_{n+1}) = Z_{n+1} \middle| Z(t_n) = Z_n, Z(t_{n-1}) = Z_{n-1}, \ldots, Z(t_1) = Z_1\right\} =$$
$$\Pr\left\{Z(t_{n+1}) = Z_{n+1} \middle| Z(t_n) = Z_n\right\}$$

ami azt jelenti, hogy a korábbi állapotokra vonatkozó pótlólagos információnak nincs befolyása arra a valószínűségre, hogy a rendszer a t_{n+1} időpontban a Z_{n+1} állapotban lesz, feltéve, hogy a t_n időpontban a Z_n állapotban volt. Ez a feltételes valószínűség tekinthető a $P_{i,j}$ átmeneti valószínűségnek, amennyiben a rendszer a t_n időpontban az $x(t_n) = i$, a következő t_{n+1} időpontban pedig az $x(t_{n+1}) = j$ állapotba került. Az átmenet feltételes valószínűsége rövid **dt** idő alatt az átmenet **intenzitás**ának (gyakoriságának, az eseménysűrűségnek) és a **dt** időtartamnak a szorzata:
A $Z_i \Rightarrow Z_j$ átmenetre: $a_{ij}(t) \cdot dt$, vagyis

$$\Pr\left\{x(t+dt) = j \middle| x(t) = i\right\} = a_{ij}(t) \cdot dt \qquad (7\text{-}67)$$

Ezt a feltételes valószínűséget a Z_i állapotban való tartózkodás valószínűségével, (a feltétel valószínűséggel) kell megszorozni. Így annak valószínűsége, hogy a rendszer a **t** időt követően **dt** idő alatt a Z_i-ből Z_j-be lép:

$$\Pr\left\{x(t)=i \wedge x(t+dt)=j\right\} = P_i(t)\cdot a_{ij}(t)\cdot dt \qquad (7\text{-}68)$$

Ha az átmenet intenzitása az időben állandó, $a_{ij}(t)=a_{ij}$, akkor a folyamatot időben homogénnek nevezzük. Fizikailag ez a megbízhatóság elméletben a nem öregedő tulajdonságot jelenti, az átmenetekhez ezért az **exponenciális eloszlás** tartozik.

$$\Pr\left\{x(t)=i \wedge x(t+dt)=j\right\} = P_i(t)\cdot a_{ij}\cdot dt \qquad (7\text{-}69)$$

Az állapotok száma gyakorlatilag véges, az egyenleteket valamennyi állapotváltozásra felírva egy differenciálegyenlet rendszer jön létre, amely megoldható, a kezdeti állapoteloszlást is számításba véve meghatározható valamennyi $\mathbf{Z_x}$ állapot $\mathbf{P_x(t)}$ valószínűsége:

$$P_j(t+dt) = \sum_{\forall x\neq j} P_x(t)\cdot a_{xj}dt + P_j(t)\cdot\left[1-\sum_{\forall x\neq j} a_{jx}dt\right] \qquad (7\text{-}70)$$

A fenti (7-70) kifejezés első tagja annak a valószínűsége, hogy a t időpontban valamelyik $Z_x \neq Z_j$ állapotban van a rendszer és dt idő alatt Z_j állapotba megy. A második tag pedig, hogy t időpontban Z_j-ben van és dt idő alatt ott is marad, tehát nem megy semelyik $Z_x \neq Z_j$ állapotba sem. Ebből átrendezés után:

$$\left(\frac{dP_j(t)}{dt} = \right)\frac{P_j(t+dt)-P_j(t)}{dt} = \sum_{\forall x\neq j} P_x(t)\cdot a_{xj} - P_j(t)\cdot\sum_{\forall x\neq j} a_{jx}dt \qquad (7\text{-}71)$$

Ha az egyenletrendszernek létezik egy stacioner megoldása, amennyiben az idő tart a végtelenhez, akkor a rendszer **„ergodikus”** és valamennyi Z_j állapotra:

$$\frac{dP_j(t)}{dt} = 0 \qquad (7\text{-}72)$$

és így a (7-71) és (7-72) összefüggések alapján:

$$\sum_{\forall x \neq j} P_x \cdot a_{xj} = P_j \cdot \sum_{\forall x \neq j} a_{jx} dt \tag{7-73}$$

ahol:

$$\lim_{t \to \infty} P_x(t) = P_x \tag{7-74}$$

A stacioner állapoteloszláshoz tartozó, **időben állandó valószínűségeket** – az egyszerűség kedvéért – **az időfüggvényükkel azonos betűvel, idő argumens nélkül jelöljük,** az a_{ij} átmeneti intenzitásokhoz hasonlóan.

Az ergodikus struktúrák az állapottér modellek egy speciális, szűkebb osztályát alkotják. Az ezek elemzésére szolgáló módszerek alkalmazhatósága korlátozott ugyan az általánosabb állapottér modellhez viszonyítva, azonban egy olyan egyszerű számítási eljárást tesznek lehetővé, ami a gyakorlatban adódó feladatok nagy részének megoldására hasznosítható.

A gyakorlatban a javított, karbantartott berendezések esetében, ha minden hibát reális időn belül tökéletesen kijavítanak és minden állapot minden állapotból (ha nem is közvetlenül) elérhető, más szóval, ha rendszer állapotterében nincs olyan zárt állapotcsoport, ami az állapotoknak csak egy részét tartalmazza és nincs ebből az állapotcsoportból kilépés, akkor teljesülnek az ergodicitási feltételek. Ilyenkor a rendszert csak tranziens állapotokat tartalmazó egyetlen összefüggő gráf modellezi. Nem tartalmaz sem forrást, sem nyelőt, sem zárt állapotcsoportot, amelybe csak belépés van, kilépés nincs.

Az elérhetőség nem jelent feltétlenül közvetlen összeköttetést, csak azt, hogy egymáshoz közvetlenül csatlakozó irányított élek folytonos sorozatával van átmenet valamennyi állapot között. Az ergodikus jelzőt a matematikai irodalomban másképpen is értelmezik.

Ha a struktúra – az előzőek szerint értelmezve – ergodikus, akkor kellően hosszú idő alatt valamennyi állapot bekövetkezik, (végtelen hosszú idő alatt biztosan valamennyi). Az idő növelésével az egyes állapotokban eltöltött (összegzett) idő monoton nő. Az időtartamok relatív értéke és ezzel az állapotok relatív valószínűsége stabilitást mutat. Minden határon túl növekvő időben stacioner valószínűség-eloszlás jön létre, amelyik a kezdeti állapot eloszlástól nem függ.

A gyakorlatban a valószínűségek időfüggvényére viszonylag ritkán van szükség, ezért továbbiakban a stacioner megoldást részletezzük, a tranziens analízisre pedig csak röviden utalunk majd a későbbiekben. Ezzel egy lineáris egyenletrendszer megoldása árán valamennyi alapvető paraméter meghatározására mód van: kiszámítható minden állapothoz és állapotcsoporthoz az abban való tartózkodás várható időtartama és stacioner valószínűsége is, azzal a feltétellel, hogy modell ergodikus. Ez utóbbi feltétel elvileg erősen korlátozza az alkalmazhatóságot, azonban a modell kis kiegészítésével valamennyi gyakorlati kérdést nem ergodikus esetre is meg tudunk válaszolni. (A differenciálegyenlet rendszer megoldása persze néha nem nélkülözhető, ezt majd a ben mutatjuk be.)

Az **ergodicitási feltétel (6)** elvileg a legerősebben korlátozó tényező.

Az állapotok valószínűsége általában az idő függvénye. Ha a meghibásodás véletlen folyamat eredménye, a jó állapotok valószínűsége – javítás nélkül – időben monoton csökkenő, redundancia-mentes elektronikus berendezésekben a legtöbbször exponenciális függvény szerinti. A hibás állapotokhoz tartozó valószínűség pedig monoton növekvő.

A jó állapotok csoportjára vonatkozóan a megfelelő P_x-ek összegét a korábbiakkal összhangban jelölhetjük **K**-val, mert ez adja a készenléti tényezőt. Meg kell rögtön jegyeznünk, hogy rövid javítási idők esetén *ez utóbbi határérték igen jó közelítést ad a* **d(t)** *időfüggvényre* (és ráadásul a biztonság irányában tér el lényegtelen mértékben a pillanatnyi értéktől), így gyakorlatilag rendszerint felesleges időfüggvényekkel számolni a lényegesen egyszerűbb konstans határértékek helyett.

7.4.3. Állapotgráf

7.4.3.1. Az állapotgráfok általános ismertetése

A többállapotú rendszerek áttekintését jól segíti egy az állapotokat és a közöttük lehetséges átmeneteket ábrázoló **gráf,** amelyben a rendszer állapotai a **gráf csúcspontjai**, az átmenetek az **irányított élek.** Az élekhez az irányon kívül intenzitásértéket is rendelünk, ezek alapján számíthatók az előzőkben felsorolt paraméterek.

Annak valószínűsége, hogy a rendszer az $X = i$ állapotból az $X = j$-be megy át egy kis **dt** idő alatt (feltéve, hogy éppen az $X = i$-ben tartózkodik):

$$P_{ij}(t,t+dt) = a_{ij} \cdot dt \cdot P_i(t) \qquad (7\text{-}75)$$

ahol a_{ij} az **i → j** átmenet intenzitása és a feltétel valószínűség $\mathbf{P_i}$. **Homogén** a Markov-folyamat, ha a $P_{ij}(t,t+dt)$ átmeneti valószínűségek nem függenek a **t** időponttól, hanem csak a **dt** időintervallumtól. Ezt a tulajdonságot az átmeneti valószínűségek stacionaritásának is szokták nevezni, ilyenkor az intervallum helyzete közömbös, csak a hossza a jellemző. Ez a tulajdonság az állandó meghibásodási ráta esetén fennáll, míg a monoton növekvő meghibásodási ráta esetén (tehát az öregedési fázisban) nem. A homogenitásra vonatkozó kikötés (5) tehát akkor áll fenn, ha az a_{ij} az időben állandó (lásd a (4-28) egyenletet a nem öregedő rendszerekkel kapcsolatban).

Ha a rendszer egyik elemének meghibásodása okozza az átmenetet, akkor az adott elem meghibásodási tényezője (λ) az intenzitás, ha javításról van szó, akkor a megfelelő intenzitás a javítási tényező, ez a javítási idő várható értékének (MTTR) reciproka, ezt μ-vel fogjuk jelölni.

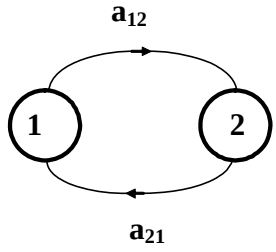
A **markovitás** (4) emlékezet mentességet jelent: a_{ij} nem függ attól, hogy a t időpontot megelőzően milyen állapot(ok)ban volt a rendszer.

Mielőtt a számításokat ismertetnénk, bemutatjuk a legalapvetőbb struktúrák gráfjait és a tartalékolás különböző fajtáihoz tartozó gráfokat.

1. Egyszerű javítható rendszer

A rendszernek két állapota van: üzemképes (X=1) és rossz (X=2). A meghibásodás intenzitása: λ, a javításé: μ.

Az állapotátmenetek intenzitásai: $a_{12} = \lambda$; $a_{21} = \mu$ (7-20. ábra).



7-20. ábra: Javítható rendszer állapot gráfja

2. Javítható 3-tagú soros rendszer

A soros rendszer három egységének meghibásodási tényezője sorra: λ_1, λ_2, λ_3, a javítás intenzitása: μ (7-21. ábra). Az állapotátmenetek intenzitásai: $a_{12} = \lambda_1 + \lambda_2 + \lambda_3$ és $a_{21} = \mu$

3. Két különböző egységből álló redundáns rendszer

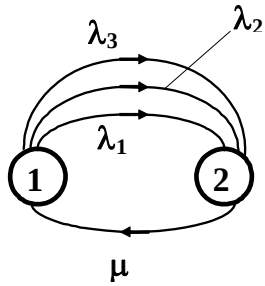
A párhuzamos (redundáns) rendszer két egységének (a és b) meghibásodási tényezője: λ_a , λ_b (7-22. ábra). A rendszernek négy állapota van:

X=1 : mindkét egység jó,
X=2 : az a egység rossz,
X=3 : a b egység rossz,
X=4 : mindkét egység rossz.

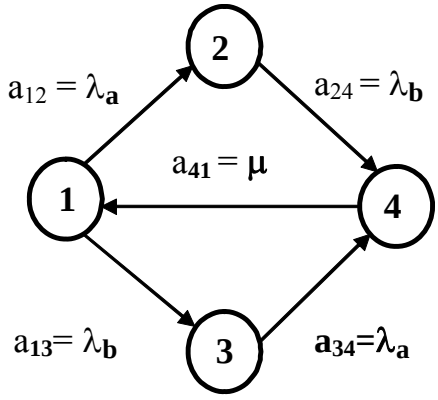
Javítás csak akkor van, ha rendszer üzemképtelenné vált (**X=4**)

Az állapotátmenetek intenzitásai:

$a_{12} = \lambda_a$, $a_{13} = \lambda_b$, $a_{24} = \lambda_b$, $a_{34} = \lambda_a$, $a_{41} = \mu$



7-21. ábra: Javítható soros rendszer állapot gráfja



7-22. ábra: Javítható párhuzamos rendszer állapot gráfja (1)

4. Két egyforma egységből álló javított redundáns rendszer

Az előző párhuzamos rendszer két egységének egyenlő a meghibásodási tényezője: $\lambda_a = \lambda_b = \lambda$, a javítás hasonló maradt.

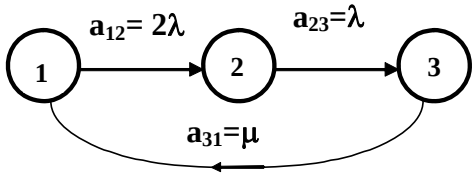
Most három állapotot különböztethetünk meg:

X=1 : mindkét egység jó.

X=2 : valamelyik egység rossz.

X=3 : mindkettő rossz.

Az állapotátmenetek intenzitásai: $a_{12} = 2\lambda$, $a_{23} = \lambda$, $a_{31} = \mu$ a 7-23. ábra szerint.



7-23. ábra: Forró tartalékolt javítható rendszer állapot gráfja

55. Stand-by rendszer (kikapcsolás nélkül)

Két egyforma λ meghibásodási tényezőjű operatív és egy λ k meghibásodási tényezőjű közös egység stand-by rendszert alkot. Nincs javítás.

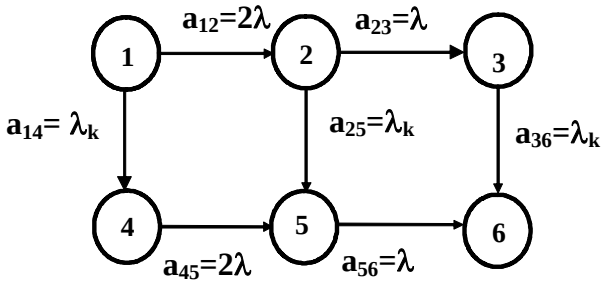
Hat állapotot értelmezünk:

X = 1 – a tökéletes jó állapot,

X = 2 – még üzemképes,

X = 3, 4, 5 és 6-ban a rendszer üzemképtelen (7-24. ábra).

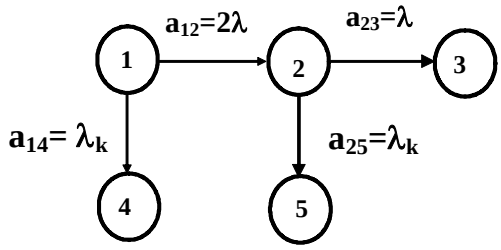
Feltétel a példa szerinti rendszerben, hogy azt nem kapcsolják ki üzemképtelenség esetén és így még további hibák is keletkezhetnek.



7-24. ábra: Stand-by rendszer állapot-gráfja (1)

Például az **X = 5** állapotban az egyik operatív egység és a közös egység rossz, de lehetséges, hogy ezután a másik operatív egység is meghibásodik: **X = 6**.
Az állapotátmenetek intenzitásai:
$\mathbf{a_{12} = a_{45} = 2\lambda,\ a_{23} = a_{56} = \lambda,\ \ a_{14} = a_{25} = a_{36} = \lambda_k}$.

6. Stand-by rendszer (kikapcsolással)
Vizsgáljuk az előzőhöz hasonló stand-by rendszert azzal a különbséggel, hogy a rendszert üzemképtelenség esetén azonnal kikapcsolják, így további meghibásodások nem léphetnek fel. Ezzel az állapotok száma eggyel, az átmenetek száma hárommal csökkent.
Az állapotátmenetek intenzitásai az előzőekhez képest:
$\mathbf{a_{36} = a_{56} = a_{45} = 0}$ a 7-25. ábra szerint



7-25. ábra: Stand-by rendszer állapot gráfja (2)

Az 1–4. pontok alatt ismertetett rendszerek ergodikusak, az 5) és 6) alattiak nem, mivel utóbbiakban nem mindegyik állapot érhető el bármelyikből. Például az **X=1** állapotból csak kilépés lehetséges, oda visszajutni csak egy javítással lehetne.

7.4.3.2. A különböző tartalékolási módok figyelembevétele

A 7.3.2.3. fejezetben említésre került a **forrótartalék**, **csökkentett terhelésű tartalék** és a **hidegtartalék** fogalma. Kanonikus modellel ezek közül csak a forrótartalék volt számítható, mivel a másik két tartalékolási mód esetében az egységek meghibásodási folyamatát befolyásolja az, hogy üzemi állapotban vannak-e, vagy tartalékként készenléti állapotban és ez az állapot megváltozhat minden meghibásodás és javítás bekövetkezésekor.

Hidegtartaléknak nevezzük azt a redundáns rendszert, amelyben teljesen kizárható az üzemen kívüli (tehát még tartalékban lévő) egység meg-

hibásodása. Más szóval a hidegtartalékban lévő egység meghibásodási tényezője csak a bekapcsolását követően nagyobb nullánál.

A hidegtartalékolt rendszer megbízhatóságának időfüggvénye a Poisson eloszlás alapján számítható. Bizonyítás nélkül ezt az eloszlást alkalmazva annak valószínűsége, hogy a **(0, t)** intervallumban éppen **h** hiba következik be:

$$P_h(t) = \left[\frac{(\lambda \cdot t)^h}{h!} \right] \cdot e^{-\lambda \cdot t} \tag{7-76}$$

Ennek alapján az **n** egységből álló hidegtartalékolt rendszer megbízhatósága, azaz annak valószínűsége, hogy a **0, t** intervallumban bekövetkező hibák száma kisebb **n**-nél:

$$R_h(t) = \sum_{k=0}^{n-1} P_k(t) = e^{-\lambda \cdot t} \cdot \sum_{k=0}^{n-1} \frac{(\lambda \cdot t)^k}{k!} \tag{7-77}$$

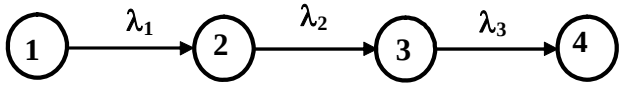
Egyébként bizonyítható az is, hogy a rendszer megbízhatatlansága (azaz hibavalószínűsége):

$$1 - R_h(t) = \sum_{k=n}^{\infty} P_k(t) \tag{7-78}$$

Folytassuk tehát az állapotgráfok előállítására vonatkozó példák sorát:

7. Hideg tartalékolás állapotgráfja

Három egységű hidegtartalékolás esetén az állapotgráf az alábbi, ha a három egység meghibásodási tényezője rendre: λ_1, λ_2 és λ_3 (7-26. ábra).



7-26. ábra: A hideg tartalékolás állapot-gráfja

Az **X=1** állapotban még valamennyi egység jó, az első működik, a többi kikapcsolt tartalék. Az **X=2** állapotba akkor kerül a rendszer, ha az első egység már meghibásodott és a második működik. A harmadik állapotban

(**X=3**) az utolsó egység még jó, a negyedikben (**X=4**) a rendszer üzemképtelen. A példánk szerinti esetben nincs javítás.

8. Hideg tartalékolás egyforma egységek esetén

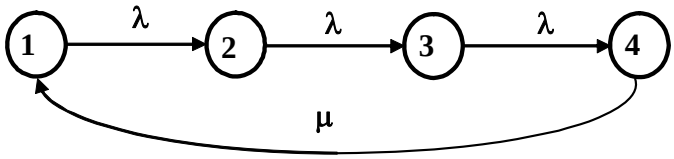
Ha az előző hidegtartalékolt rendszer egységei egyformák: azaz

$$\lambda_1 = \lambda_2 = \lambda_3 = \lambda$$

Amennyiben csak akkor javítanak, ha a rendszer már üzemképtelenné vált és a javítás teljes felújítás, a gráf a 7-27. ábra szerint alakul. Ebben az esetben minden egység átlagosan

$$T = \frac{1}{\lambda}$$

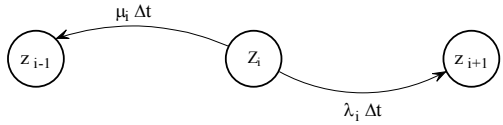
ideig működőképes.



7-27. ábra: Javítható hideg tartalékolt rendszer állapot-gráfja

9. Születési-halálozási folyamat állapotgráfja

Születési-halálozási folyamatnak nevezik a modellt, ha a gráfban csak a szomszédos állapotokba van átmenet. Ezek a sztochasztikus folyamatok speciális osztályát képezik, amelyek a kiszolgálás elméletben, készletgazdálkodási problémáknál és a megbízhatósági vizsgálatoknál egyaránt fontos szerepet játszanak. A folyamat állapotát ezeknél születés (érkezés, javítás) és halál (távozás, meghibásodás) egyaránt megváltoztathatja (7-28. ábra).

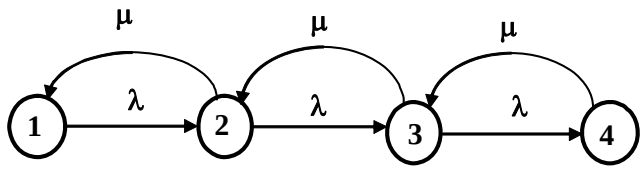


7-28. ábra: Születési halálozási folyamat

Egy diszkrét Markov-folyamatot születési-halálozási folyamatnak nevezünk, ha a következő feltételek fennállnak: a folyamat $\lambda_i \cdot dt$ valószínűséggel jut a Z_i állapotból a Z_{i+1} állapotba és $\mu_i \cdot dt$ valószínűséggel a Z_i

állapotból a Z_{i-1} állapotba. Az állapotváltozás során a dt -nek elegendően kicsinynek kell lenni, hogy feltételezhessük, hogy egy időben két esemény nem következik be. Ha $\lambda_i = 0$, akkor tiszta születési, ha $\mu_i = 0$, akkor pedig tiszta halálozási folyamatról beszélünk.

Az alábbi példa egy ilyen hidegtartalékolt rendszer „egyenként javítással" (7-29. ábra). A példában három egyforma egység van, a javítások intenzitása is egyenlő. Az X=1 állapot a tökéletes, az X=4 állapotban a rendszer üzemképtelen.

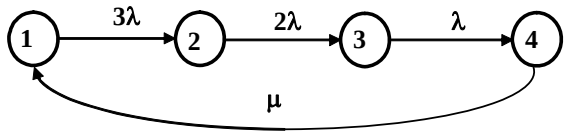


7-29. ábra: Születési-halálozási folyamat állapot-gráfja

10. Javítható forrótartalékolt rendszer

Forrótartaléknak nevezzük azt a redundáns rendszert, amelyben az egységek meghibásodását nem befolyásolja, hogy funkcionálnak, vagy tartalékban vannak. A meghibásodási tényezőjük nem függ más egységek állapotától.

A 8. pont szerinti háromegységes rendszer forrótartalékolva az alábbi gráffal modellezhető (7-30. ábra). Az **X=1** állapotban mindhárom egység jó, egyik teljesíti a rendszer funkcióját, a másik kettő bekapcsolt tartalék. Az átmenet intenzitása $\mathbf{a_{12}= 3\lambda}$. Ezután az **X=2**-ben már egy egység kiesett, az **X=3**-ban pedig az utolsó egység funkcionál.



7-30. ábra: Javítható forró tartalékolt rendszer állapot-gráfja

Nem biztos azonban, hogy a tartalékban lévő egység meghibásodása kizárható (tehát nem igazán **hideg** a tartalékolás), ugyanakkor az is gyakori, hogy a tartalék a kisebb stressz következtében kisebb meghibásodási té-

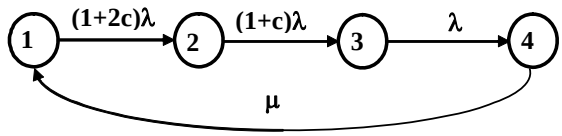
nyezőjű, mint a funkcionáló egység, (tehát a tartalékolás nem is igazán forró).

11. Csökkentett igénybevételű tartalék

Csökkentett igénybevételű tartalék az a redundancia forma, amelynél a tartalékos egységek meghibásodása nem zárható ki, de kisebb gyakoriságú, mint a funkcionálóé, tehát kisebb, mint a forrótartalék esetén. Ilyenkor például bekapcsolt állapotban lehet a tartalék egység, de nincs terhelése és ezért kisebb a meghibásodási tényezője.

A forró és a hidegtartalékolás szélsőséges közelítései a valóságnak, a most tárgyalt köztes eset kissé bonyolultabban modellezhető, de gyakran jobban írja le a rendszert.

Legyen a tartalékban lévő egység meghibásodási tényezője **cλ,** ahol az üzemelő egység meghibásodási tényezője **λ** és a **0<c<1.** Könnyen belátható, hogy **c = 0** a hidegtartalék, **c = 1** a forrótartalék esete, tehát a csökkentett terhelésű tartaléknak a két szélsőséges változat speciális esetei. A példa szerint az **X=1** állapotban egy egység (az első) működik és kettő tartalék. A három közül bármelyik meghibásodásának következménye az **X=2** állapot. Itt már csak egy tartalék maradt és egy újabb meghibásodás eredménye az **X=3** állapot, ahol nincs tartalék és az utolsó egység működik. Most a 7-31. ábra szerinti a gráf.



7-31. ábra: Javítható csökkentett terhelésű tartalékolt rendszer állapot-gráfja

Összefoglalásként az N egyforma egységből párhuzamos struktúrával felépülő rendszerekre vonatkozó átmeneti intenzitásokat az alábbi 7-1. táblázat tartalmazza. Itt is λ a meghibásodási tényező, λ' pedig a csökkentett terhelésre érvényes érték.

Az előzőekben megismert példák alapján könnyen értelmezhetők az alábbi állapotfajták:

Állapot sorszáma	Hibás egységek száma	Átmeneti intenzitás	Forró tartalék	Hideg tartalék	Csökkentett terhelés
1	0	$a_{1,2}$	$N \cdot \lambda$	λ	$\lambda + (N-1) \cdot \lambda'$
2	1	$a_{2,3}$	$(N-1) \cdot \lambda$	λ	$\lambda + (N-2) \cdot \lambda'$
3	2	$a_{3,4}$	$(N-2) \cdot \lambda$	λ	$\lambda + (N-3) \cdot \lambda'$
…	…	…	…	…	…
n	N-1	$a_{n,n+1}$	λ	λ	λ
n+1	N	-	0	0	0

7-1. táblázat: Különböző tartalékolási módok jellemzői

- **Tranziens** az állapot, ha az állapotba van belépés és van belőle kilépés is. Ilyen a 1., 2., 3. és 4. esetre vonatkozó állapotgráf valamennyi állapota.
- **Szomszédos** két állapot, ha egy lépéssel egyikből a másik elérhető. Az összes példánkban ilyen az **X=1** és az **X=2**
- **Összekötött** két állapot ha a kettő közül bármelyik bármelyikből elérhető. A 4. eset állapotgráfjában mindhárom állapot ilyen.
- **Forrás** az olyan állapot, amelyikből csak kilépés van, belépés nincs. A 5. és 6. esetekre vonatkozó állapotgráfban ilyen az **X=1.**
- **Nyelő** az olyan állapot, amelyikbe csak belépés van, kilépés belőle nincs. Az 5. esetre vonatkozó állapotgráfban az **X=6**, a 6. esetén az **X=3,4,5.** Fizikailag nyelő csak hibás állapot lehet, hiszen ellenkező esetben valami örökké jó maradna, ami gyakorlatilag kizárt.

7.4.4. Állapotidő

Az előzőekben részletesen megvizsgáltuk az állapotok közötti átmenetek kérdését. A megbízhatóság vizsgálat során további fontos kérdés, hogy várhatóan mennyi ideig tartózkodik a rendszer az egyes állapotokban.

A $\mathbf{Z}_i$ állapotban várhatóan $\mathbf{T}_i$ ideig tartózkodik a rendszer. Ha $\mathbf{Z}_i$-ből csak egy állapotba, $\mathbf{Z}_j$-be van átmenet, akkor:

$$T_i = \frac{1}{a_{ij}} \tag{7-79}$$

ha több állapotba van átmenet, akkor az intenzitások összegének reciprok értéke a várható tartózkodási idő:

$$T_i = \frac{1}{\sum_j a_{ij}} \tag{7-80}$$

(Emlékezzünk a 4.2 fejezetben az exponenciális eloszlásról írottakra, valamint a (4-26) képletre.)

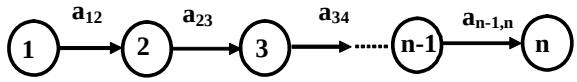
7-24. példa

Egy háromegységes soros rendszer egységeinek meghibásodási tényezője sorra: $\lambda_A, \lambda_B, \lambda_C$. Az eredő: $\lambda_S = \lambda_A + \lambda_B + \lambda_C$ és ezzel: $T_{FS} = \frac{1}{\lambda_S}$

✸

Elágazás nélküli gráf (7-32. ábra) esetén az eredő várható időtartam a részidőtartamok összege:

$$T_F = \frac{1}{a_{12}} + \frac{1}{a_{23}} + \frac{1}{a_{34}} + \ldots + \frac{1}{a_{n-1,n}} \tag{7-81}$$

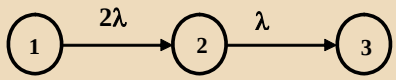


7-32. ábra: Elágazás nélküli állapotgráf

7-25. példa

Tekintsük az egyszerű kétegységes (7-33. ábra szerint javítás nélküli forró-tartalékolt) rendszert.

Felírható a rendszer üzemképtelenségéig várható működési idő a (7-90) egyenlet felhasználásával: $T_F = \frac{1}{a_{12}} + \frac{1}{a_{23}}$, ami a felsorolt három tartalékolási esetben:



7-33. ábra: Kétegységes forró tartalékolt rendszer

a) forró tartalék: $T_{FF} = \frac{1}{2\lambda} + \frac{1}{\lambda} = \frac{3}{2} \cdot T$

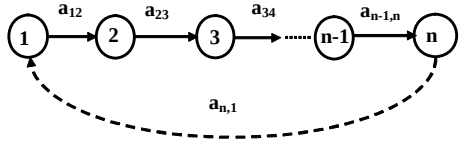
b) hideg tartalék: $T_{FH} = \frac{1}{\lambda} + \frac{1}{\lambda} = 2 \cdot T$

c) csökkentett terhelésű tartalék: $T_{FC} = \frac{1}{\lambda} + \frac{1}{\left(\lambda + \lambda'\right)} = \left[1 + \frac{\lambda}{\lambda + \lambda'}\right] T$

ahol $T = \frac{1}{\lambda}$ az egység várható jó működési ideje.

Ha javítás csak rendszerhiba esetén van (7-34. ábra) és az teljes felújítást jelent, akkor $T_F = T_U$ és $T_D = \frac{1}{a_{n,1}}$. A készenléti tényező is számítható:

$$K = \frac{T_U}{T_U + T_D}$$



7-34. ábra: Rendszerhiba esetén teljes felújítás

7.4.5. Megbízhatósági számítások

A számításokat az alábbi (bizonyítás nélkül közölt) szabályok és összefüggések alapján végezhetjük el. A jobb áttekinthetőség kedvéért itt összefoglaljuk a számításokhoz szükséges korábban ismertetetteket is.

Az állapotok indexe **x = 1, 2, … h, … m.** A korábbiak szerint a rendszer üzemképes, ha $1 \le x \le h$ és üzemképtelen, ha $h < x \le m$.

I.

A (7-69) egyenletnek megfelelően az **x =i** állapotból az **x =j**-be való átmenet valószínűsége igen kis **Δt** idő alatt

$$a_{ij} \cdot P_i(t) \cdot \Delta t \tag{7-82}$$

ahol $\mathbf{a_{ij}}$ az átmenet intenzitása és

$$P_i(t) = \Pr\{x(t) = i\} \tag{7-83}$$

II.
A $\mathbf{P_x(t)}$ valószínűségek összege minden időpillanatban egységnyi

$$\sum_{x=1}^{m} P_x(t) = 1, \qquad \mathrm{x} = 1, 2, \ldots \mathrm{m} \tag{7-84}$$

III.
Az **ergodikus** rendszerben nem lehet sem forrás, sem nyelő állapot, sőt forrás vagy nyelő jellegű állapotcsoport sem lehet benne. A valóságban azonban vannak nem javított berendezések is és ezek struktúrája természetesen nem ergodikus. Az analízis ezekre a rendszerekre a megismert eszközökkel oly módon végezhető el, hogy **átmeneti jelleggel** extrém paraméterű javítást értelmezünk és ezzel ergodikussá tesszük. Az ergodicitásból adódóan létezik az állapotoknak egy határeloszlása, ahol

$$P_x = \lim_{t \to \infty} \mathrm{P_x}(t) \tag{7-85}$$

III/a
Valamennyi állapot stacioner valószínűsége nagyobb nullánál:

$$P_x > 0 \qquad \forall x \tag{7-86}$$

III/b
A $\mathbf{Z_i}$ állapot $\mathbf{P_i}$ stacioner valószínűsége számítható a stabilitásból adódó egyensúly feltételből: e szerint az állapotba való belépéseknek a kilépésekkel egyensúlyt kell tartaniuk, mert különben az adott állapot valószínűsége hosszú idő alatt vagy a nullához, vagy az egységhez tartana, ez viszont csak forrás, illetve nyelő esetén lenne lehetséges, ilyen viszont az ergodikus rendszerben nincs. Tehát ha az állapotgráfot tetszés szerinti helyen kettévágjuk, a vágás helyét átmetsző intenzitások **egyensúly**t tartanak. A vágás

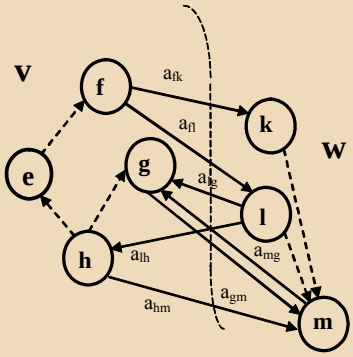
révén létrejött két diszjunkt állapotcsoporthoz tartozó indexek halmazát jelölje v és w, amelyre: $\{v\} \wedge \{w\} = \Phi; \quad \{v\} \vee \{w\} = \Omega$

$$\sum_{\forall i \in v} \left[P_i \sum_{\forall j \in w} a_{ij} \right] = \sum_{\forall j \in w} \left[P_j \sum_{\forall i \in v} a_{ji} \right] \tag{7-87}$$

Ebből az egyensúlyi egyenletből valamennyi állapot stacioner valószínűsége számítható:

$$P_j = \frac{\sum_{\forall j \in w} \left[P_x \sum_{\forall x \neq j} a_{xj} \right]}{\sum_{\forall x \neq j} a_{jx}} \tag{7-88}$$

7-26. példa



7-35. ábra: A stacioner állapotok egyensúlya

A III/b. szabály illusztrálására példaként szolgál a fenti gráf (7-35. ábra), ahol a két állapotcsoporthoz tartozó állapotok

$$e, f, g, h \in v \text{ és } k, l, m \in w$$

Így az egyensúlyi egyenlet:

$$P_f \left(a_{fk} + a_{fl} \right) + P_g a_{gm} + P_h a_{hm} = P_l \left(a_{lg} + a_{lh} \right) + P_m a_{mg}$$

III/c

Az I és a III/b szabályok értelmében bármelyik **állapotra** felírható egy ilyen egyensúlyi egyenlet: az állapotból kimutató intenzitások összege egyenlő az állapotba bemutató intenzitások összegével [a (7-89) egyenlet szerint]:

$$\sum_{\forall i \neq k} P_i a_{ik} = P_k \sum_{\forall i \neq k} a_{ki} \qquad (7\text{-}89)$$

ahol **X = k** a kérdéses állapot és **i** valamennyi állapot a **k** kivételével.

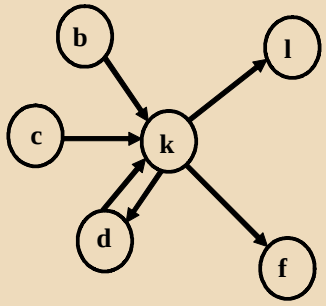
IV.

Az **állapotokban való tartózkodás várható időtartama** az állapotból kimutató átmenetek összegzett intenzitásának reciprok értéke. Az **X= i** állapotban tehát a várható időtartam:

$$T_i = \frac{1}{\sum_{\forall j \neq i} a_{ij}} \qquad (7\text{-}90)$$

7-27. példa

A III/c. szabály illusztrálására szolgál az alábbi gráf (7-36. ábra).



7-36. ábra: A k-ik állapot megváltozásai

Itt az egyenlet:

$$P_b a_{bk} + P_c a_{ck} + P_d a_{dk} = P_k \left(a_{kd} + a_{kl} + a_{kf} \right)$$

✸

IV/a.
Egy adott v állapotcsoportban való tartózkodás várható időtartama:

$$T_v = \frac{\sum_{\forall i \in v} P_i}{\sum_{\forall i \in v} \left[P_i \sum_{\forall j \notin i} a_{ij} \right]} \tag{7-91}$$

ahol $\mathbf{a_{ij}}$ a v állapotcsoportból kimutató átmenetek intenzitása ($v \subset \Omega, \quad i \in v, \quad j \notin v$).

IV/b.
Az előzőből adódik, hogy a rendszer **üzemképes állapotához tartozó várható idő**

$$T_u = \frac{K}{\sum_{\forall i \le h} \left[P_i \sum_{\forall j > h} a_{ij} \right]} \tag{7-92}$$

ahol **K** a készenléti tényező és **h** a hibakorlát, ami a (4-5) és (4-6) összefüggések szerint értelmezendő.

V.
A rendszer **készenléti tényező**je az üzemképes állapotban való tartózkodás stacioner valószínűsége, tehát a az adott állapotok valószínűségének összege.

$$\mathrm{K} = \sum_{\forall \mathrm{i} \le \mathrm{h}} \mathrm{P_i} \tag{7-93}$$

A szabályok alkalmazásának bemutatására közöljük a fentiekben a 7.4.3 fejezetben szereplő rendszerekre vonatkozó számításokat és eredményeket. Egyes esetekben ismertetjük a számítás közbenső eredményeit is.

7-28. példa: A legegyszerűbb kétállapotú rendszer

A 7-20. ábra szerinti rendszerre a készenléti tényező: $K = \frac{\mu}{\lambda + \mu}$. Két meghibásodás között várható jó működési idő: $T_U = \frac{1}{\lambda}$

✸

7-29. példa: Háromegységes soros rendszer

A 7-21. ábra szerinti rendszerre az eredő meghibásodási tényező

$$\lambda_S = \lambda_1 + \lambda_2 + \lambda_3$$

A készenléti tényező: $K = \dfrac{\mu}{\lambda_S + \mu}$

Két meghibásodás között várható jó működési idő $T_U = \dfrac{1}{\lambda_S}$

✸

7-30. példa: Kétegységes forrótartalékolt rendszer

A 7-22. ábra szerinti rendszerre:

$$P_1(\lambda_a + \lambda_b) = P_4 \cdot \mu \qquad P_1 = \frac{\mu \cdot \lambda_a \cdot \lambda_b}{A}$$

$$P_1.\lambda_a = P_2.\lambda_b \qquad P_2 = \frac{\mu \cdot \lambda_a^2}{A}$$

$$P_1.\lambda_b = P_3.\lambda_a \qquad P_3 = \frac{\mu \cdot \lambda_b^2}{A}$$

$$P_1 + P_2 + P_3 + P_4 = 1 \qquad P_4 = \frac{\lambda_a \cdot \lambda_b \cdot (\lambda_a + \lambda_b)}{A}$$

ahol a közös nevező:

$$A = \mu \cdot \lambda_a \cdot \lambda_b + \mu \cdot (\lambda_a^2 + \lambda_b^2) + \lambda_a \cdot \lambda_b \cdot (\lambda_a + \lambda_b)$$

Készenléti tényező:

$$K = P_1 + P_2 + P_3 = \frac{\mu \cdot (\lambda_a \cdot \lambda_b + \lambda_a^2 + \lambda_b^2)}{A}$$

Két meghibásodás között várható jó működési idő:

$$T_U = \frac{K}{P_2 \cdot \lambda_b + P_3 \cdot \lambda_a} = \frac{\lambda_a \cdot \lambda_b + \lambda_a^2 + \lambda_b^2}{\lambda_a^2 \cdot \lambda_b + \lambda_b^2 \cdot \lambda_a}$$

✸

4-20. példa: Két egyforma egységből álló forrótartalékolt rendszer

A 7-23. ábra szerinti rendszerre:

$$P_2 = P_1 \cdot \frac{2\lambda}{\lambda} = 2 \cdot P_1 \qquad P_1 = \frac{\mu}{3\mu + 2\lambda}$$

$$P_3 = P_2 \cdot \frac{\lambda}{\mu} = 2 \cdot P_1 \cdot \frac{\lambda}{\mu} \qquad P_2 = \frac{2\mu}{3\mu + 2\lambda}$$

$$P_1\left[1 + 2 + \frac{2\lambda}{\mu}\right] = 1 \qquad P_3 = \frac{2\lambda}{3\mu + 2\lambda}$$

$$P_1 + P_2 + P_3 = 1$$

Készenléti tényező:

$$K = P_1 + P_2 = \frac{3\mu}{3\mu + 2\lambda}$$

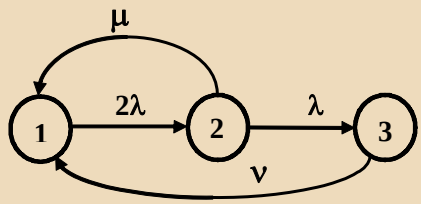
Két meghibásodás között várható jó működési idő:

$$T_U = \frac{K}{P_2 \cdot \lambda} = \frac{3}{2\lambda}$$

✸

7-31. példa: Az előző rendszer másféle javítási politikával (7-37. ábra)

A hibás, de még üzemképes (**X=2**) állapotból μ intenzitással ($1/\mu$ várható javítási idővel) hárítják el a hibát. A rendszer üzemképtelen (**X=3**) állapotából a helyreállítás intenzitása **ν**. A modellben alkalmazott két különböző intenzitású javítás lehetőséget ad arra, hogy a gyakorlatban eltérő javításpolitikákat írjanak elő (például a gyakorlatban a **ν > μ** esettel a sürgős hibaelhárítás modellezhető, vagy a **ν = 0** esettel egy olyan rendszer írható le, amelyet üzemképtelenség esetén nem javítanak stb.)



7-37. ábra: Javítható, két egységes forró tartalékolt rendszer állapotgráfja

$$P_1 \cdot 2\lambda = P_2(\mu + \lambda) \qquad P_2 \cdot \lambda = P_3 \cdot \nu$$

$$P_1 = \frac{(\mu + \lambda)\cdot \nu}{A} \qquad P_2 = \frac{2\lambda \cdot \nu}{A}$$

$$P_3 = \frac{2\lambda^2}{A} \qquad P_1 + P_2 + P_3 = 1$$

ahol $A = \mu \cdot \nu + 3\lambda \cdot \nu \cdot \mu$

Készenléti tényező:

$$K = P_1 + P_2 = \frac{\mu \cdot \nu + 3\lambda \cdot \nu \cdot \mu}{\mu \cdot \nu + 3\lambda \cdot \nu \cdot \mu + 2\lambda^2}$$

Két meghibásodás között várható jó működési idő:

$$T_U = \frac{P_1 + P_2}{P_2 \cdot \lambda} = \frac{\frac{3}{2} + \frac{\mu}{2\lambda}}{\lambda}$$

✸

7-32. példa: Hidegtartalékolás

A 7-26. ábra szerinti rendszerre a rendszer üzemképtelenné válásáig várható jó működési idő: $T_F = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \frac{1}{\lambda_3}$

A stacioner állapotvalószínűségek számításának itt nincs értelme, hiszen ez a rendszer nem ergodikus. A (7-72) egyenlet alapján az **n** egységből álló hidegtartalékolt rendszer megbízhatósága, azaz annak valószínűsége, hogy a **(0, t)** intervallumban bekövetkező hibák száma kisebb **n**-nél:

$$R_H(t) = \sum_{k=0}^{n-1} P_k(t) = e^{-\lambda \cdot t} \sum_{k=0}^{n-1} \frac{(\lambda \cdot t)^k}{k!}$$

Egyébként bizonyítható az is, hogy a rendszer megbízhatatlansága:

$$1 - R_H(t) = \sum_{k=n}^{\infty} P_k(t)$$

7-33. példa: Három egyforma egységű hidegtartalékolt rendszer

A 7-27. ábra szerinti rendszer esetén minden egység átlagosan T = 1/λ ideig működőképes, tehát ez a hidegtartalékolt rendszer javítás nélkül

$$T_F = \frac{3}{\lambda} = 3T$$

ideig jó. A készenléti tényező egyszerűen is kiszámítható:

$$K = \frac{3\mu}{3\mu + \lambda}$$

De az állapottér modellel is felírható:

$$P_1 \cdot \lambda = P_2 \cdot \lambda = P_3 \cdot \lambda = P_4 \cdot \mu$$

$$P_1 = P_2 = P_3 = \frac{\mu}{3\mu + \lambda} \qquad P_4 = \frac{\lambda}{3\mu + \lambda}$$

$$P_1 + P_2 + P_3 + P_4 = 1$$

$$P_1\left[3 + \frac{\lambda}{\mu}\right] = 1$$

Természetesen a két meghibásodás között várható jó működési időre is a fenti eredmény adódik: $T_U = \frac{3}{\lambda}$

✸

7-34. példa: Hidegtartalékolás egyenkénti javítással

A 7-29. ábra szerinti rendszer esetén:

$$P_1 \cdot \lambda = P_2 \cdot \mu \qquad P_1 = \frac{1}{A}$$

$$P_2 \cdot \lambda = P_3 \cdot \mu \qquad P_2 = \frac{\alpha}{A}$$

$$P_3 \cdot \lambda = P_4 \cdot \mu \qquad P_2 = \frac{\alpha^2}{A}$$

$$\alpha = \frac{\lambda}{\mu} \qquad P_2 = \frac{\alpha^3}{A}$$

$$P_1 + P_2 + P_3 + P_4 = 1$$

$$A = 1 + \alpha + \alpha^2 + \alpha^3$$

Készenléti tényező:

$$K = P_1 + P_2 + P_3 = \frac{1+\alpha+\alpha^2}{1+\alpha+\alpha^2+\alpha^3}$$

Két meghibásodás között várható jó működési idő:

$$T_U = \frac{K}{P_3 \cdot \lambda} = \frac{1+\alpha+\alpha^2}{\alpha^2 \cdot \lambda}$$

✸

7-35. példa: Forrótartalékolt rendszer

A 7-30. ábra szerinti rendszer esetén

$P_1 \cdot 3\lambda = P_2 \cdot 2\lambda = P_3 \cdot \lambda = P_4 \cdot \mu$

$P_1 + P_2 + P_3 + P_4 = 1$

$P_1 = \frac{2}{A}$ $\quad P_3 = \frac{6}{A}$

$P_2 = \frac{3}{A}$ $\quad P_4 = 6 \cdot \frac{\lambda}{\mu} \cdot \frac{1}{A}$

$A = 11 + 6 \cdot \frac{\lambda}{\mu}$

Készenléti tényező:

$$K = P_1 + P_2 + P_3 = \frac{11}{A}$$

Két meghibásodás között várható jó működési idő:

$$T_U = \frac{1}{3\lambda} + \frac{1}{2\lambda} + \frac{1}{\lambda} = \frac{11}{6\lambda}$$

Azaz a három forrótartalékban működő egység még a kétszeresét sem teljesíti az egység várható élettartamának, a hidegtartalék – mint láttuk – az egység élettartamának háromszorosát szolgáltatta, tehát sokkal előnyösebb a forrótartaléknál, ha **valóban realizálható** a hidegtartalékolás.

✸

7-36. példa: Csökkentett terhelésű rendszer

A 7-31. ábra szerinti rendszer esetén

$$P_1 \cdot \lambda \cdot (1+2c) = P_2 \cdot (1+c) = P_3 \cdot \lambda = P_4 \cdot \mu$$

$$P_2 = P_1 \cdot \frac{1+2c}{1+c} \qquad P_1 = \frac{1+c}{A}$$

$$P_3 = P_1 \cdot (1+2c) \qquad P_2 = \frac{1+2c}{A}$$

$$P_4 = P_1 \cdot \frac{\lambda}{\mu} \cdot (1+2c) \qquad P_3 = \frac{(1+c)\cdot(1+2c)}{A}$$

$$P_1 + P_2 + P_3 + P_4 = 1 \qquad P_4 = \frac{\lambda}{\mu} \cdot \frac{(1+c)\cdot(1+2c)}{A}$$

$$A = 2 + 3c + \left[1 + \frac{\lambda}{\mu}\right] \cdot (1 + 3c + c^2)$$

Készenléti tényező:

$$K = P_1 + P_2 + P_3 = \frac{[(1+c)+(1+2c)+(1+c)\cdot(1+2c)]}{A}$$

Két meghibásodás között várható jó működési idő:

$$T_U = \frac{K}{P_3 \cdot \lambda} = \frac{(1+c)+(1+2c)+(1+c)\cdot(1+2c)}{\lambda \cdot (1+c)\cdot(1+2c)}$$

✸

7-37. példa: Háromegységes javított majoritásos rendszer

A 7.3.4 fejezetben ismertettük ezt a struktúrát (a (7-8. ábra), illetve (7-50) egyenlet):

$$R_{rendszer}(t) = R_{LE}(t) \cdot R_{majoritás}(t)$$

ahol az egyes operatív egységek megbízhatósága: $R(t) = e^{-\lambda \cdot t}$,

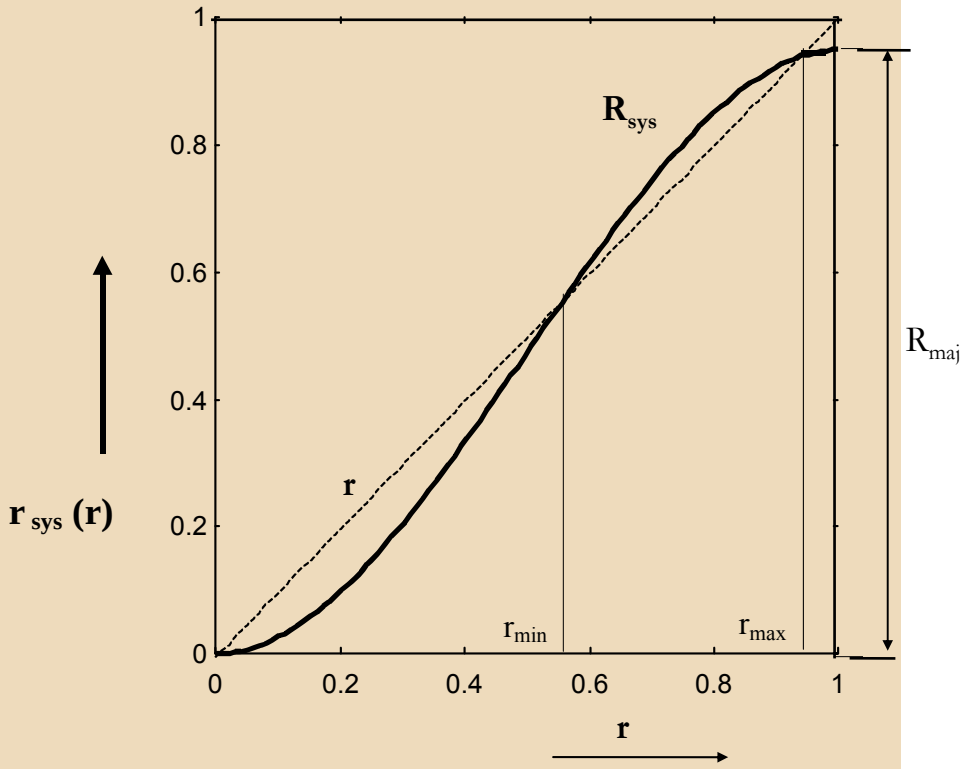
és a redundáns operatív rész (a hibamentes állapotban többségben működő egységek) megbízhatósága: $R_{majoritás}(t) = 3R^2(t) - 2R^3(t)$

A szavazó logikai egység megbízhatósága:

$$R_{LE}(t) = e^{-\lambda_{LE} \cdot t}$$

Így $R_{rendszer}(t) = 3 \cdot e^{-(2\lambda+\lambda_{LE})\cdot t} - 2 \cdot e^{-(3\lambda+\lambda_{LE})\cdot t}$ (7-38. ábra).A várható működési idő kiszámításának képlete egy integrált tartalmaz. (Lásd a 2.3.2. fejezet 2-27. képletét.)

$$T = \int_0^{\infty} R(t) \cdot dt$$



7-38. ábra: A majoritásos rendszer megbízhatósága az operatív egység megbízhatóságának függvényében

Az integrandusok formája ezekben a megbízhatósági számításokban rendszerint az alábbihoz hasonló:

$$T = \int_0^{\infty} a \cdot e^{-bt} \cdot dt = \frac{a}{b} \cdot \left[e^{-bt} \right]_0^{\infty} = \frac{a}{b}$$

Ebben az esetben is ez az előző forma adódik, így az eredmény:

$$\mathbf{T_{rendszer}} = \frac{5\lambda + \lambda_{LE}}{(2\lambda + \lambda_{LE}) \cdot (3\lambda + \lambda_{LE})}$$

Ha a szavazó logikai egység tökéletesen hibamentesnek tekinthető, azaz $\lambda_{LE} = 0$, akkor

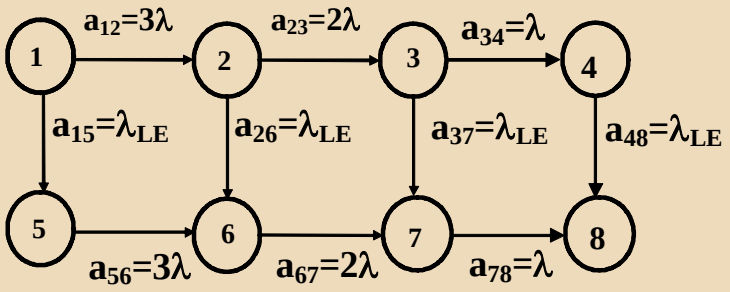
$$R_{majoritás}(t) = 3 \cdot e^{-2\lambda \cdot t} - 2 \cdot e^{-3\lambda \cdot t} \text{ és } T_{majoritás} = \frac{3}{2\lambda} - \frac{2}{3\lambda} = \frac{5}{6\lambda} < \frac{1}{\lambda}$$

Tehát még ebben az ideális esetben is kisebb az ilyen három egységből felépített redundáns rendszernek a várható élettartama, mint egyetlen egységé. Javított, nagy megbízhatóságú rendszerekben és rövid működtetésű idejű nem javított berendezésekben mégis érdemes ilyen struktúrákat alkalmazni, mivel – ha a javítás nélkül várható működési idő kisebb is – de lényegesen kedvezőbb a jó működés valószínűsége, azaz nagyobb a megbízhatóság adott ideig, mint egyetlen egységé.

✸

7-38. példa: Állapottér modell alkalmazása

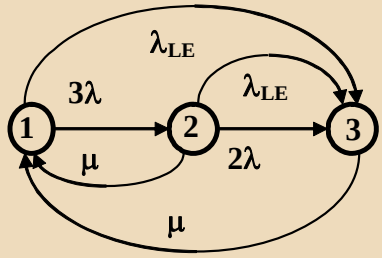
Az előző feladat állapottér modellel is megoldható. A háromegységes javítás nélküli majoritásos rendszer állapotgráfját arra az esetre, amikor a rendszert meghibásodás esetén nem kapcsoljuk ki, a 7-39. ábra mutatja.



7-39. ábra: Majoritás logikával működő rendszer állapotgráfja

Itt **λ** az operatív egységek meghibásodási tényezője, λ_{LE} pedig a logikáé. Csak az **X=1** és **X=2** állapot üzemképes a rendszer, az **X= 3…8** üzemképtelen.

Ha a rendszert hibás állapotban kikapcsolják és minden hibát teljes felújítással javítanak, akkor a 7-40. ábra szerinti az állapotgráf. (Itt is csak az **X=1** és **X=2** állapot üzemképes.)



7-40. ábra: Majoritás logikával működő javított rendszer állapotgráfja

Az egyenletek:

$$P_1(3\lambda + \lambda_m) = P_2\mu + P_3\mu$$
$$P_2(2\lambda + \lambda_m) + P_1 \cdot \lambda_m = P_3\mu$$
$$P_1 + P_2 + P_3 = 1$$

A készenléti tényező

$$K = P_1 + P_2 = \frac{\mu \cdot (5\lambda + \lambda_{LE} + \mu)}{(3\lambda + \lambda_{LE} + \mu) \cdot (2\lambda + \lambda_{LE} + \mu)}$$

Két meghibásodás között várható jó működési idő

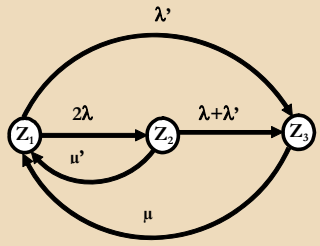
$$T_U = \frac{K}{P_3 \cdot \lambda_{LE} + P_2 \cdot (2\lambda + \lambda_{LE})}$$

✸

7-39. példa: Közös részrendszert tartalmazó forró tartalékolt rendszer

Két egyenlő (λ) meghibásodási tényezőjű egység párhuzamos forrótartalékolt részrendszert képez, amit egy λ' meghibásodási tényezőjű közös részrendszer (átkapcsoló és tápegység) egészít ki rendszerré (7-41. ábra). Hibás, de még üzemképes a rendszer, ha csak az egyik párhuzamos egység

nem működik, a közös (soros) részrendszer meghibásodása a rendszer üzemképtelenség eredményezi. Ez esetben **μ** intenzitással helyreállítják a rendszert, de a hibás de még üzemképes állapotban is van javítás egy kisebb, μ' intenzitással.



7-41. ábra: Speciális rendszer általános átmeneti intenzitásokkal

A gráf alapján felírható egyenletek a következők:

$$P_1 \cdot 2\lambda = P_2 \cdot \left(\lambda + \lambda' + \mu'\right)$$
$$P_3 \cdot \mu = P_2 \cdot \left(\lambda + \lambda'\right) + P_1 \cdot \lambda'$$
$$P_1 + P_2 + P_3 = 1$$

Az egyenletrendszer megoldása pedig:

$$P_1 = \frac{\mu \cdot \left(\lambda + \lambda' + \mu\right)}{N}$$
$$P_2 = \frac{2 \cdot \lambda \cdot \mu}{N}$$

ahol a közös nevező:

$$N = 2 \cdot \lambda^2 + 3 \cdot \lambda \cdot \lambda' + \lambda'^2 + 2 \cdot \lambda \cdot \mu + \mu \cdot \mu' + \lambda' \cdot \mu'$$

A két meghibásodás közt várható jó működési idő:

$$T_U = \frac{\left(P_1 + P_2\right)}{\left[P_1 \cdot \lambda' + P_2 \cdot \left(\lambda + \lambda'\right)\right]}$$

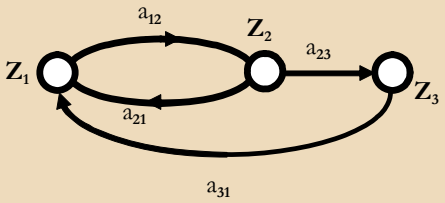
vagy az eredmények felhasználásával:

$$T_U = \frac{3\cdot\lambda + \lambda^{'} + \mu}{\left(3\cdot\lambda\cdot\lambda^{'} + 2\cdot\lambda^{2} + \lambda^{'2} + \lambda^{'}\cdot\mu^{'}\right)}$$

✸

7-40. példa

A 7-42. ábra gráfjával ábrázolt ergodikus rendszer **K** és $\mathbf{T_U}$ számítása általánosan értelmezett átmeneti intenzitásokkal az alábbi. Két gyakorlati relációja az *A)* és a *B)* pont szerinti.



7-42. ábra: Állapotgráf általános átmeneti intenzitásokkal

A gráf alapján felírható egyenletek:

$$P_1 a_{12} = P_2 a_{21} + P_3 a_{31} \qquad P_2 a_{23} = P_3 a_{31}$$
$$P_1 a_{12} = P_2\left(a_{21} + a_{23}\right) \qquad P_1 + P_1 + P_1 = 1$$

Az egyenletrendszer megoldásával az egyes állapotvalószínűségek:

$$P_1 = \frac{\left(a_{21} + a_{23}\right)\cdot a_{31}}{\left(a_{21} + a_{23}\right)\cdot a_{31} + \left(a_{23} + a_{31}\right)\cdot a_{12}}$$

$$P_2 = \frac{a_{12}\cdot a_{31}}{\left(a_{21} + a_{23}\right)\cdot a_{31} + \left(a_{23} + a_{31}\right)\cdot a_{12}}$$

$$P_3 = \frac{a_{12}\cdot a_{23}}{\left(a_{21} + a_{23}\right)\cdot a_{31} + \left(a_{23} + a_{31}\right)\cdot a_{12}}$$

A rendszer készenléti tényezője:

$$K = P_1 + P_2 = \frac{\left(a_{21} + a_{23} + a_{12}\right)\cdot a_{31}}{\left(a_{21} + a_{23}\right)\cdot a_{31} + \left(a_{23} + a_{31}\right)\cdot a_{12}}$$

és a meghibásodások közt várható jó működési idő:

$$T_U = \frac{(P_1 + P_2)}{P_2 \cdot a_{31}} = \frac{(a_{21} + a_{23} + a_{12})}{a_{12} \cdot a_{23}}$$

A)

Kétegységes forrótartalékolt (rész)rendszer, hiba esetén üzemképes állapotban ν intenzitással javítják, üzemképtelen állapotban felújítják μ intenzitással. Így az állapotátmenetek intenzitásai:

$$a_{12} = 2\lambda; \quad a_{21} = \nu; \quad a_{23} = \lambda; \quad a_{31} = \mu;$$

Ezt felhasználva a készenléti tényező és a várható jó működési idő:

$$K = \frac{3\lambda + \nu}{\left[\mu \cdot (3\lambda + \nu) + 2\lambda^2\right]} \quad \text{és} \quad T_U = \frac{3\lambda + \nu}{2\lambda^2}$$

B)

Egy távoli ország utjain bárhol előfordulhatnak szegek, amelyek átlagosan Δl = 1000 km távolságonként autógumi defektet okoznak. Persze vannak gumijavítók mindenütt az országban átlagosan s = 10 kilométerenként. Az autónk egy pótkerékkel rendelkezik (ami teljes értékű, a csomagtartóban van, biztonságban, azaz hidegtartalékot képez). Milyen gyakorisággal (M km távolságonként) kell autómentőt hívni, mivel már a pótkerék is kilyukadt, mielőtt az első lyukat az első gumijavítónál kijavíttattuk volna? (Érdemes lenne-e két pótkereket hurcolni?) Ebben az esetben az intenzitások: $a_{12} = a_{23} = \frac{1}{l}; \quad a_{21} = \frac{1}{g}; \quad a_{31} \to 0$

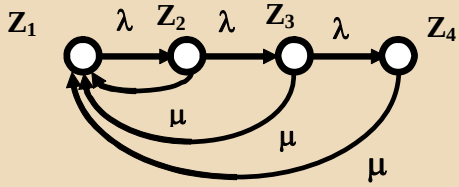
és a keresett távolság: $M = l \cdot \left(2 + \frac{l}{g}\right) = 1000(2 + 100) = 102.000[km]$

✸

7-41. példa:

Egy jól karbantartott, három egyforma, λ meghibásodási tényezőjű egységből álló hidegtartalékolt (rész)rendszer gráfja az alábbi (7-43. ábra). Itt a jó karbantartás alatt az értendő, hogy minden hibás állapotból egyforma μ intenzitással javítanak és a javítás minden esetben teljes felújítás. Számít-

suk ki a **K** készenléti tényezőt és a két rendszerhiba közötti várható $\mathbf{T_U}$ jó működési időt.



7-43. ábra: Jól karbantartott hidegtartalékolt rendszer

Az egyenletrendszert a következőképpen állíthatjuk fel:

$$P_1 \cdot \lambda = P_2 \cdot (\lambda + \mu) \qquad P_3 \cdot \lambda = P_4 \cdot \mu$$
$$P_2 \cdot \lambda = P_3 \cdot (\lambda + \mu) \qquad P_1 + P_2 + P_3 + P_4 = 1$$

A megoldások pedig:

$$P_1 = \frac{\mu \cdot (\lambda + \mu)^2}{N} \qquad P_3 = \frac{\lambda^2 \cdot \mu}{N}$$
$$P_2 = \frac{(\lambda + \mu) \cdot \lambda \cdot \mu}{N} \qquad P_4 = \frac{\lambda^3}{N}$$

ahol

$$N = (\lambda + \mu) \cdot (2\lambda + \mu) \cdot \mu + \lambda^2 \cdot (\lambda + \mu)$$

Ezzel a **K** készenléti tényező és a két rendszerhiba közötti várható $\mathbf{T_U}$ jó működési idő:

$$K = P_1 + P_2 + P_3 = \frac{(\lambda + \mu) \cdot (2\lambda + \mu) \cdot \mu + \lambda^2 \cdot \mu + \lambda \cdot \mu}{N}$$

$$T_U = \frac{(\lambda + \mu) \cdot (2\lambda + \mu) + \lambda^2}{\lambda^3}$$

✸

7.4.6. Nem ergodikus rendszerek

Nem ergodikus a rendszer, ha tartalmaz

- **forrás** vagy **nyelő** állapotot, vagy
- **zárt állapotcsoportot,** amelybe van belépés és nincs belőle kilépés.

A nem ergodikus rendszer a stacioner állapoteloszlásra triviális eredményeket adna: a forrás állapotra és a tranziens állapotokra 0 valószínűséget, a nyelőre (pontosabban a nyelők összegére) pedig 1 valószínűséget. A számítások a tranziens analízis módszerével, a megfelelő differenciál egyenletek megoldásával elvégezhetők, azonban számos esetben van lehetőség az egyszerűbb stacioner analízis eredményeinek felhasználására.

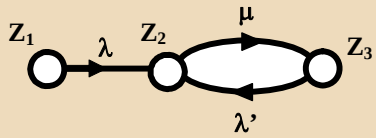
Két módszert mutatunk be az alábbi példákkal:

- az állapotgráf szétválasztása,
- fiktív helyreállítás alkalmazása.

Ezek a módszerek a példáknál bonyolultabb (több állapotú) modellekre is alkalmazhatók.

7-42. példa: Egyszerű nem ergodikus rendszer vizsgálata

A készüléket meghibásodás esetén javítják, azonban a javítás eredményeként kisebb megbízhatóságú lesz. Az új készlék meghibásodási tényezője: λ, a javításokkal a meghibásodási tényező λ'-re nő, a javítási tényező: μ (7-44. ábra).



7-44. ábra: Nem ergodikus modell

$\mathbf{Z_1}$ a kezdeti állapot, amikor a meghibásodási tényező λ. $\mathbf{Z_2}$ az üzemképtelen állapot, $\mathbf{Z_3}$ a már megjavított, amelyből $\lambda'>\lambda$ meghibásodási tényezővel romlik el a készülék.
Közvetlenül belátható, hogy itt

$$T_F = \frac{1}{\lambda}, \qquad T_U = \frac{1}{\lambda'}, \qquad K = \frac{\mu}{\mu + \lambda'}$$

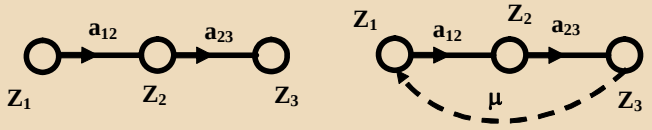
✸

Amennyiben az üzemképtelen állapot(ok) nyelő(k), a modell nem ergodikus, de ilyen esetekben rendszerint alkalmazhatunk egy a valóságban

nem létező fiktív felújítást, ahol a javítás intenzitása: $\mu \to 0$, azaz $T_D \to \infty$. A modell ergodikussá válik és a meghibásodásig várható idő számítható. Ezen kívül sok ilyen készülék átlagára értelmezhetően a jó állapotok relatív valószínűsége is meghatározható.

7-43. példa: Kétegységes redundáns rendszer

A rendszer két egységes redundáns(7-45. ábra).



7-45. ábra: Kétegységes redundáns rendszer

Triviális, hogy ha $\boldsymbol{\mu \to 0}$, akkor $\mathbf{P_1 \to 0}$ és $\mathbf{P_2 \to 0}$ és $\mathbf{P_3 \to 1}$, de $\mathbf{T_F}$ és sok ilyen rendszer átlagára értelmezhetően a $\mathbf{P_1/P_2}$ arány számítható:

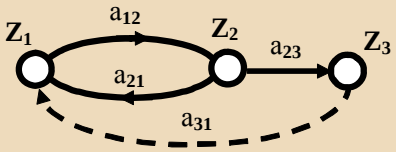
Az egyenletek: $P_1 \cdot a_{12} = P_2 \cdot a_{23} = P_3 \cdot \mu$ továbbá $P_1 + P_2 + P_3 = 1$

Ezekből: $\frac{P_2}{P_1} = \frac{a_{12}}{a_{23}}$ és $T_U = \frac{P_1 + P_2}{P_2 \cdot a_{23}} = \frac{a_{12} + a_{23}}{a_{12} \cdot a_{23}} \left(= \frac{1}{a_{12}} + \frac{1}{a_{23}} \right)$, amely eredmény összhangban van az korábbiakkal.

✸

7-44. példa

Hasonlóan számítható egy olyan rendszer is, amelyekben javítások vannak. (Itt az $\mathbf{a_{31}}$ egy fiktív javítás. De az $\mathbf{a_{21}}$ miatt az egyszerűbb módszerekkel nem tudtuk elvégezni a számításokat.)



7-46. ábra: Nem ergodikus rendszer fiktív javítással

A $\mathbf{T_U}$ értékét a 7-42. ábra kapcsán a alapján már meghatároztuk

7.4.7. Tranziens analízis

Az állapot valószínűségek időfüggvényére szükség van tervszerű (időben periodikus, vagy adott kockázathoz tartozó) javításokkal üzemeltetett rendszerek, valamint adott időtartamú „küldetések" megbízhatóságának kiszámításához. Tehát olyan esetekben, ha a megbízhatóság időfüggvényét alapul véve adott megbízhatatlansághoz tartozó időpontot, vagy adott időponthoz tartozó megbízhatóságot kell kiszámítani. A karbantartás nélküli kanonikus és a hidegtartalékolt modellek esetében az állapotvalószínűségek időfüggvényét a korábbi fejezetekben felírtuk, de szélesebb körben, például ha eseménykövető javítások is vannak, akkor az eddig tárgyalt módszerek nem tették lehetővé az időfüggvények meghatározását.

Az időfüggvények kiszámíthatók az állapottér alapján felírható differenciál egyenletrendszer megoldásával. Az analízis részletes ismertetése meghaladja a könyv korlátjait, de a Laplace transzformációt alkalmazni tudó olvasóknak néhány kisebb terjedelmű példával illusztráljuk az eljárás lényegét. A gyakorlatban szokásos, mátrixokat is használó és ezzel nagyfokú tömörséget (és eleganciát) adó módszer részletesebb ismertetését mellőztük.

A feladat megoldása az alábbi lépésekben lehetséges:

1. differencia egyenletek felállítása,
2. áttérés a differenciál egyenletekre,
3. mátrixos írásmódra való áttérés,
4. gyakorlati következtetések levonása.

A fenti lépéseket egy egyszerű példán mutatjuk be. Tekintsük ismét a 7-33. ábra szerinti forró tartalékolt, javítás nélküli párhuzamos rendszert.

ad 1. **A differencia egyenletek felállítása**

Az egyenletek felállításának alapja a $P_i(0)$ kezdeti eloszlás ismerete. Minden vizsgálatnál kezdeti állapotként a $t = 0$ időpontbeli állapotot vesszük figyelembe. Ez nem előfeltétel, de megkönnyíti az érhetőséget. (Más kezdeti időpontot speciális vizsgálatok esetén szoktak figyelembe venni.) További kiindulási feltétel, hogy a rendszer a kezdeti időpontban a hibátlan, működőképes állapotban van. Ebből következik erre az időpontra vonatkozóan, hogy

$$P_1(0) = 1; \qquad P_2(0) = 0; \qquad P_3(0) = 0$$

Feltételezzük, hogy tetszőleges **t** időpontban ismert a rendszer állapota és keresett a rendszer állapota a későbbi **t+Δt** időpontban. A **Δt** időtartamnak olyan kicsinek kell lennie, hogy ezen belül csak egy állapotváltozás legyen. A $\mathbf{Z_1}$ állapottal kapcsolatban keressük annak a valószínűségét, hogy **t+Δt** időpontban a rendszer még mindig hibátlan. A hibátlan állapot valószínűsége az idővel egyre csökken. Mivel nincs javítás, **t+Δt** időpontban csak akkor lehet jó a rendszer, ha a **t**-időpontban is az volt! Ezt a valószínűséget csökkenti az a lehetőség, hogy éppen a következő Δt idő alatt hibásodik meg a rendszer:

$$P_1(t+\Delta t) = P_1(t) - P_1(t)\cdot a_{12}\cdot \Delta t \qquad (7\text{-}94)$$

Az átmeneti intenzitás az említett ábra alapján:

$$a_{12} = 2\lambda$$

A kapott egyenletből a függvény növekményét a következőképpen fejezhetjük ki:

$$\frac{P_1(t+\Delta t) - P_1(t)}{\Delta t} = -2\lambda \cdot P_1(t) \qquad (7\text{-}95)$$

A $\mathbf{Z_2}$ állapottal kapcsolatban keresett annak a valószínűsége, hogy (**t+Δt**) időpontban 1 hiba van a rendszerben. Ezzel kapcsolatban a következő lehetőségek adódnak:

- a **t** időpontban jó **(Z_1)** és **Δt** alatt meghibásodik
- a **t** időpontban már a **Z2** állapotban van
- a **Z2**-ben maradás valószínűségét csökkenti, ha éppen a következő **Δt** idő alatt hibásodik meg a második részrendszer

Ezt a következő módon fejezhetjük ki:

$$\begin{aligned} &P_2\left(t+\Delta t\right) = P_2(t) + a_{12}\cdot\Delta t\cdot P_1(t) - a_{23}\cdot\Delta t\cdot P_2(t) = \\ &2\lambda\cdot\Delta t\cdot P_1(t) + \left(1-\lambda\cdot\Delta t\right)\cdot P_2(t) \end{aligned} \qquad (7\text{-}96)$$

A kapott egyenletből a függvény növekményét a következőképpen fejezhetjük ki:

$$\frac{P_2(t+\Delta t)-P_2(t)}{\Delta t}=2\lambda\cdot P_1(t)-\lambda\cdot P_2(t) \qquad (7\text{-}97)$$

A $\mathbf{Z_3}$ állapottal kapcsolatban keresett annak a valószínűsége, hogy (t+Δt) időpontban 2 hiba van a rendszerben. Lehetőségek:

- t időpontban a rendszer már üzemképtelen, vagyis a $\mathbf{Z_3}$ állapotban van
- t időpontban a rendszer még a $\mathbf{Z_2}$ állapotban van (csak 1 hiba), de **Δt** alatt újabb meghibásodás jelentkezik

$$P_3(t+\Delta t)=P_3(t)+a_{23}\cdot\Delta t\cdot P_2(t)=P_3(t)+\lambda\cdot\Delta t\cdot P_2(t) \qquad (7\text{-}98)$$

A kapott egyenletből a függvény növekményét a következőképpen fejezhetjük ki:

$$\frac{P_3(t+\Delta t)-P_3(t)}{\Delta t}=\lambda\cdot P_2(t) \qquad (7\text{-}99)$$

ad 2. **Átmenet differencia egyenletről differenciálegyenletre**
Az egyes állapotvalószínűségekre kapott differenciahányadosokból a szokásos határátmenet feltételezésével kapjuk a differenciálhányadosokat. A $\mathbf{Z_1}$ állapotra vonatkozóan:

$$P_1'(t)=\frac{dP_1}{dt}=\lim_{\Delta t\to 0}\frac{P_1(t+\Delta t)-P_1(t)}{\Delta t}=-2\lambda\cdot P_1(t) \qquad (7\text{-}100)$$

A többi állapotfüggvényre vonatkozóan hasonlóan eljárva kapjuk a Markov gráfra vonatkozó differenciálegyenlet-rendszert:

$$\begin{aligned} P_1'(t)&=-2\lambda\cdot P_1(t)\\ P_2'(t)&=2\lambda\cdot P_1(t)-\lambda\cdot P_2(t)\\ P_3'(t)&=\lambda\cdot P_2(t)\end{aligned} \qquad (7\text{-}101)$$

Feladat ezen állandó együtthatós elsőrendű differenciál-egyenletrendszer megoldása, ami célszerűen Laplace transzformáció alkalmazásával végezhető. Ez, mint ismeretes, az eredeti függvényt egy képfüggvénybe viszi át a következők szerint. A szokásos jelölések:

- a Laplace transzformációra: $L\{P(t)\}=P(s)$

- a deriváltra: $$L\left\{\frac{dP_i(t)}{dt}\right\} = s \cdot P_i(s) - P_i(t=0)$$
- a kezdőállapot pedig: $P_1(0) = 1$ és $P_i(0) = 0 \quad \forall i>1$

Tehát esetünkben:

$$s \cdot P_1(s) - 1 = -2\lambda \cdot P_1(s) \tag{7-102}$$

$$s \cdot P_2(s) = 2\lambda \cdot P_1(s) - \lambda \cdot P_2(s) \tag{7-103}$$

$$s \cdot P_3(s) = \lambda \cdot P_2(s) \tag{7-104}$$

Az egyenletrendszer megoldása ebben az egyszerű esetben azonnal adódik, hisz a (7-102) egyenletből $\mathbf{P_1}$ kifejezhető:

$$P_1(s) = \frac{1}{s+2\lambda},$$

a (7-103)-ból:

$$P_2(s) = \frac{2\lambda}{s+\lambda} \cdot P_1(s) = \frac{2\lambda}{s+\lambda} \cdot \frac{1}{s+2\lambda} = \frac{2\lambda}{(s+\lambda)\cdot(s+2\lambda)}$$

s végül a (7-104)-ből:

$$P_3(s) = \frac{\lambda}{s} \cdot P_2(s) = \frac{\lambda}{s} \cdot \frac{2\lambda}{(s+\lambda)\cdot(s+2\lambda)} = \frac{2\lambda^2}{s\cdot(s+\lambda)\cdot(s+2\lambda)}$$

A fenti megoldások alapján az egyes állapotvalószínűségek időfüggvénye inverz-Laplace transzformációval adódnak. A szükséges transzformációs képletek (7-2. táblázat):

$p(s)$	$p(t)$
$\frac{Z}{s+a}$	$Z \cdot e^{-at}$
$\frac{Z}{(s+a)\cdot(s+b)}$	$Z \cdot \frac{e^{-bt} - e^{-at}}{a-b}$

$\frac{Z}{s\cdot(s+a)\cdot(s+b)}$	$Z\cdot\left(\frac{1}{a\cdot b}+\frac{b\cdot e^{-bt}-a\cdot e^{-at}}{a\cdot b\cdot(a-b)}\right)$

7-2. táblázat: Laplace transzformáció

Ezek felhasználásával:

$$P_1(t)=e^{-2\lambda\cdot t}$$

$$P_2(t)=2\lambda\cdot\frac{e^{-2\lambda\cdot t}-e^{-\lambda\cdot t}}{\lambda-2\lambda}=2\cdot\left(e^{-\lambda\cdot t}-e^{-2\lambda\cdot t}\right)$$

$$P_3(t)=2\lambda^2\cdot\left[\frac{1}{2\lambda^2}+\frac{2\lambda\cdot e^{-\lambda\cdot t}-\lambda\cdot e^{-2\lambda\cdot t}}{2\lambda^2\cdot(-\lambda)}\right]=\frac{\lambda-2\lambda\cdot e^{-\lambda\cdot t}+\lambda\cdot e^{-2\lambda\cdot t}}{\lambda}=$$

$$=1-2\cdot e^{-\lambda\cdot t}+e^{-2\lambda\cdot t}$$

A fenti egyenletek alapján a párhuzamos rendszer megbízhatósági függvénye:

$$R_p(t)=P_1(t)+P_2(t)=e^{-2\lambda\cdot t}+2\cdot\left(e^{-\lambda\cdot t}-e^{-2\lambda\cdot t}\right)=$$

$$=2\cdot e^{-\lambda\cdot t}-e^{-2\lambda\cdot t}$$

és meghibásodási függvénye:

$$F_p(t)=1-2\cdot e^{-\lambda\cdot t}+e^{-2\lambda\cdot t}$$

Ellenőrizhetően teljesül az 1-es komplemens tulajdonság és az eredmény megegyezik a Boole módszer alkalmazásával korábban kapottal (7-32).

8. A biztonsággal kapcsolatos alapfogalmak

8.1. Általános megjegyzések

A bevezető fejezetben röviden szó esett már a biztonságról, annak köznapi jelentéséről, minőségben betöltött általános szerepéről. A különböző műszaki részterületeken többféle értelmezés és definíció ismeretes., a következőkben erről adunk áttekintést.

8.2. A biztonság meghatározása a meghibásodások következménye alapján

8.2.1. Általános megjegyzések

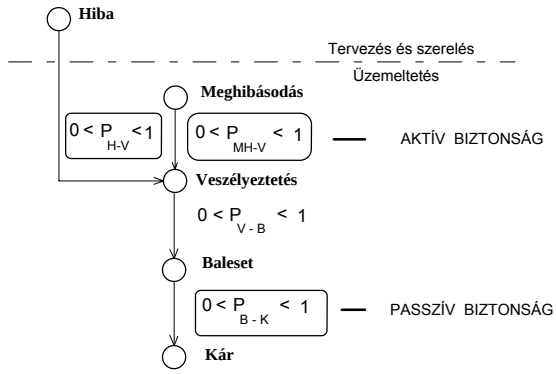
A **biztonság**ot általában egy veszélymentes állapotnak tekintjük, amellyel garantálható, hogy a rendszerrel kapcsolatban ne jelentkezzen kár. A kár a kialakult gyakorlat szerint a rendszerrel kapcsolatban lévő emberekben és tárgyakban jelentkező veszteség, melynek nagysága valamilyen természetes mutatóban (az embert érintő kár esetében haláleset, súlyos és könnyű sérülés mennyiségével, az anyagiakat érintő kár esetén pedig pénzben) fejezhető ki.

Ahogy az 1. fejezetben szó esett róla, a biztonság kérdésénél is a rendszerek hibáiból, meghibásodásaiból indulunk ki. A hiba és meghibásodás valamint a bekövetkezett kár között az alábbi ábrán bemutatott eseménylánchoz megfelelő kapcsolat van (8-1. ábra).

A hibák és meghibásodások bizonyos valószínűséggel veszélyeztetéshez vezetnek. Az ábra szerint ez a valószínűség $P_{H\text{-}V}$, illetve $P_{MH\text{-}V}$. A **veszély** az az állapot, amelyből személy és/vagy tárgy számára kár keletkezhet. A **veszélyeztetés** olyan veszélyhez vezető potenciális lehetőség, melynek fajtáját, nagyságát és irányát meghatározhatjuk.

A veszélyeztetés irányával kapcsolatban a biztonság két alapvető értelmezési lehetősége adódik, ami a magyar terminológia szerint nem válik el egymástól, de feltétlenül figyelembe veendő. Ilyen módon az angolszász irodalmakban szokásos módon beszélhetünk **„safety”** és **„security”** értelmében vett biztonságról. Előbbi esetben a biztonságkritikus rendszerből kiinduló veszélyeztetések elkerülésén van a hangsúly, míg utóbbi-

ban a biztonságkritikus rendszert kell védeni a kívülről jelentkező veszélyeztetésekkel szemben. Komplex biztonsági szemléletmód, illetve nagy veszélypotenciálú (például atomerőművi, speciális közlekedési) rendszerek esetén mindkettő figyelembevétele szükséges.



8-1. ábra: A biztonsággal kapcsolatos eseménylánc

A veszélyeztetésből bizonyos $P_{V\text{-}B}$ valószínűséggel következhet be **baleset,** például egy vonat közeledésekor le nem záródó sorompó potenciális veszélyhelyzetet jelent, de baleset csak akkor következik be, ha éppen ebben az időben a közúton is közlekedik egy jármű. Ez a valószínűség a műszaki rendszer kialakításától nem, csak a pillanatnyi forgalmi helyzettől függ.

A bekövetkezett baleset ismét bizonyos $P_{B\text{-}K}$ valószínűséggel okoz kárt, a kár nagysága azonban már esetleg függ a balesetet elszenvedő rendszer(ek) megfelelő kialakításától. A veszélyeztetések elkerülésére hozott intézkedések jelentik az aktív, a kár nagyságának korlátozására hozottak pedig az ún. passzív biztonsági intézkedéseket. Az **aktív biztonsági intézkedés**ekkel az említett valószínűségek közül a $P_{H\text{-}V}$ és $P_{MH\text{-}V}$ értékeit tarthatjuk megfelelően kis értéken, a **passzív biztonsági intézkedés**ek eredménye pedig a $P_{B\text{-}K}$ valószínűség csökkenése lehet. A $P_{V\text{-}B}$ valószínűség a rendszer műszaki kialakítási módjával nem befolyásolható, ez egyéb tényezőktől függ.

A biztonság tehát másképp fogalmazva az objektumnak az a tulajdonsága, hogy működése közben, sőt működésképtelen állapotban sem okoz veszélyt emberre, a szolgáltatás kiesésén, csökkenésén kívül nem okoz anyagi természetű kárt. Persze utóbbiak is rögzített környezeti feltételekkel, adott időtartamra vonatkoztathatók.

8.2.2. A biztonság és megbízhatóság kapcsolata

Az objektum (ezen belül főleg a biztonságkritikus berendezések és szolgáltatások) **biztonsága** nem azonos a megbízhatósággal. A biztonsági feltételek teljesítése adott esetben szigorúbb, más esetben lazább követelményeket jelent, mint a megbízhatóságé. Például egy folyamatirányító rendszer lehet kifogástalanul működőképes (tehát megbízhatóság szempontjából jó), miközben bizonyos tartalékait (redundanciáit) már elvesztette és emiatt kevésbé biztonságos. De lehet, hogy ez a rendszer miközben működésképtelenné vált (tehát megbízhatóság szempontjából rossz), a folyamatot azonban szabályosan leállította, vagy korlátozta, így a biztonság még megmaradt (bár a rendszer által felügyelt folyamat leállt, vagy kisebb teljesítményű lett). Valamely közlekedési eszköz lehet biztonságos és mégis kevéssé megbízható (például egy olyan autó, amely nehezen indítható). Hasonlóan előfordulhat, hogy egy közlekedési eszköz nagy megbízhatóságú, de nem biztonságos (például az autó nagyon ritkán hibásodik meg, de egy meghatározott meghibásodás esetén, például egy egyszerűen kivitelezett fékrendszer esetén közvetlen veszélyhelyzet lép fel. Ilyen esetben tehát állandóan aggódhat az autó tulajdonosa, hogy nehogy ez a meghibásodás lépjen fel).

A megbízhatóság és a biztonság általában nem egymásnak ellentmondó követelmény. A nagyobb megbízhatóság általában nagyobb biztonságot eredményez, de a biztonság növelése esetleg csökkentheti is a megbízhatóságot. Szolgáljanak erre példaként a következők.

1. Egy háztartási gép biztonságát növeli, ha védőföldeléssel és a tápvezetékben túláram-biztosítóval (például olvadó biztosíték) látják el, mivel így testzárlat esetén nem okoz áramütést. A biztosíték azonban meghibásodhat (például érintkezési hibája miatt nem működik a készülék). Tehát a biztosíték nem növeli, sőt csökkenti a megbízhatóságot, miközben a biztonságot hatékonyan javíthatja.
2. Kissé bonyolultabb példaként nézzünk egy olyan közúti forgalomirányító rendszert, amelyik egy adott típusú meghibásodás esetén egyszerre adna szabad jelzést két keresztező útiránynak és ezért rendkívül balesetveszélyes lenne. A biztonság növelésére kiegészíthető a rendszer egy olyan további egységgel, amelyik az adott hiba bekövetkezésekor mindkét irányba a szabad helyett egy figyelmeztető jelzést ad. Ez utóbbi azonban növeli a rendszer bonyolultságát, alkatrész-számát, méretét és emiatt a tökéletesen hibamentes működés valószínűsége, azaz a megbízhatóság csökken, bár a biztonság növekedett.

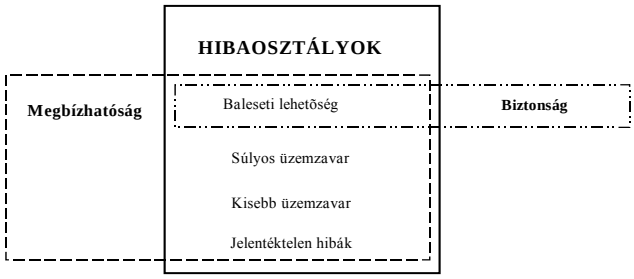
Az utóbbihoz hasonló, vagy még bonyolultabb rendszerek esetében nem egyértelmű az, hogy mit tekintünk rossz állapotnak. Mint a megbízhatósággal kapcsolatos rendszer-analízissel foglalkozó részben láttuk, az ilyen rendszerekre célszerű több hibás állapotot, többféle hibakritériumot értelmezni. Ezzel a módszerrel a megbízhatóság számítási eljárások alkalmassá válnak a biztonság paramétereinek becslésére. **A követelményeket illetően a biztonság az elsődlegesen meghatározó, az ehhez szükséges analízist és szintézist viszont a megbízhatóság módszereivel végezhetjük.**

A 2.1. fejezetben részletesen ismertettük a megbízhatósággal kapcsolatos alapvető fogalmakat, azok definícióját, befolyásoló tényezőit. A biztonság a közismert köznapi értelmén túl a biztonságelmélet alapvető kiinduló fogalmát jelenti. Sok esetben helytelenül a megbízhatósággal szinte azonos fogalomnak tekintik: minden hasonlóság ellenére alapvető különbségnek kell tekintenünk azt a tényt, hogy a biztonságelmélet területén, a biztonság megítélésére a vizsgált objektumoknak pusztán a veszélyeztetést okozó hibákat, meghibásodásokat vesszük figyelembe. A következő 8-1. táblázat mutatja a fogalmak hasonlóságát és különbségét.

A biztonság/megbízhatóság fogalmának	
hasonlósága	**különbözősége**
Mindkét fogalom hibákkal, meghibásodásokkal kapcsolatos	Megbízhatóság vizsgálatánál valamennyi hibát (akadályozó/veszélyes) figyelembe kell venni
Mindkét fogalom az adott időpontbeli hibátlan állapot valószínűségét jelenti	Biztonság vizsgálatnál csak a veszélyes hibát kell figyelembe venni

8-1. táblázat: Biztonság és megbízhatóság összehasonlítása

Heurisztikusan felvett hibaosztályok alapján egy lehetséges módon szemléltethetjük a megbízhatóság és biztonság-elmélet hibaszemléletének különbségét (lásd a 8-2. ábra).



8-2. ábra: A biztonsági és megbízhatósági vizsgálatok hibaszemlélete

8.2.3. A biztonság számjellemzői

8.2.3.1. A számjellemzők meghatározásának matematikai problémái

A veszélyeztetés-mentesség értelmében vett biztonság számszerűen azt az **S(t)** valószínűséget jelenti, hogy adott t időpontig nem jelentkezik veszélyes hiba.

A biztonsági vizsgálatok során a hibáknak/meghibásodásoknak csak egy – a veszélyeztetést okozó – részét vesszük figyelembe. Az erre vonatkozó gyakorlat szerint a pontos matematikai vizsgálat helyett bizonyos elhanyagolásokkal, közelítésekkel élünk, s a meghibásodási rátákat a veszélyeztetést okozó hibák/meghibásodások arányában redukáljuk a következők szerint.

Tekintsük az **n** egységből álló soros rendszert, melynek egyes alkatrészeire vonatkozóan ismerjük az **i** meghibásodási ráta értékét. (Itt **i** jelenti az alkatrészre jellemző index értéket). Minden egyes alkatrész-meghibásodással kapcsolatban megvizsgálható, hogy az veszélyeztető vagy akadályozó hatású lesz-e? Ha a veszélyes meghibásodások részaránya α_i (ami értelemszerűen 0 és 1 közötti szám lehet), akkor a veszélyes meghibásodásokra vonatkozó redukált meghibásodási ráta értéke a következőképpen kapható:

$$\lambda_i' = \alpha_i \cdot \lambda_i \qquad (8\text{-}1)$$

Az összefüggésben szereplő mennyiségekre vonatkozóan fennállnak a következő összefüggések:

$$0 \le \alpha_i \le 1 \text{ és } 0 \le \lambda_i' \le \lambda_i$$

Ha speciális esetként a számításba vett meghibásodások nem okoznak veszélyeztetést, akkor $\lambda_i^{'} = 0$, ha pedig minden meghibásodás veszélyes, akkor $\lambda_i^{'} = \lambda_i$, vagyis a két meghibásodási ráta megegyezik egymással. Ez a hibaredukciós módszer veszi figyelembe, hogy a rendszer nem minden meghibásodása, hanem azoknak csupán egy része veszélyes. A rendszer biztonsága növelhető, ha a veszélyes hibák részarányát csökkenteni sikerül.

A biztonsági vizsgálatok során a fenti hibaredukció alapján a biztonságkritikus rendszert is célszerűen állandó meghibásodási rátájú soros helyettesítő képpel modellezzük és a Boole modell alapján továbbra is a kétállapotú rendszrekre vonatkozó összefüggéseket alkalmazzuk. Így a rendszer veszélyes meghibásodásokra vonatkozó meghibásodási rátája (az ún. **veszélyeztetési ráta**) a komponensek rátáinak összegeként adódik. Ez a módszer matematikailag igen egyszerű, de nem tekinthető teljesen korrektnek. A pontosabb vizsgálat esetén Markov modellel lehetne figyelembe venni, hogy a rendszer állapotainak száma három (hibátlan, akadályozó és veszélyes hibás állapot!) Az a feltételezés sem helytálló, hogy a veszélyeztetési ráta, mint redukált meghibásodási ráta is egy az alkatrész veszélyes meghibásodási viselkedését jellemző exponenciális élettartam eloszlás paraméterének tekinthető. A veszélyes hibák bekövetkezésének valószínűsége ugyanis nem az 1 értékhez tart, hanem az 1-nél kisebb redukált α_i értékhez:

$$\alpha_i = \frac{\lambda_i^{'}}{\lambda_i} \leq 1 \qquad (8\text{-}2)$$

ilyen módon ez a függvény már nem tekinthető szigorú matematikai értelemben eloszlás függvénynek. A gyakorlatban előforduló esetekben azonban általában igaz, hogy:

- a megbízhatóság vizsgálat ideje általában sokkal rövidebb, mint az alkatrészre jellemző MTBF érték (a $\lambda_i \cdot t < 0,1$ értékig a relatív hiba maximum 11%, így a közelítés elfogadhatónak tekinthető),
- javítható rendszerek esetén az átlagos javítási idő (MTTR) sokkal kisebb, mint az átlagos meghibásodási időköz (MTBF). A közelítés pontossága általában megfelelő, ha a meghibásodási ráta értékére $\lambda_i < 10^{-3}$ **[1/ó]** és a javítási rátára $\mu_i > 10^{-2}$ **[1/ó]** érvényes.
- Periodikus fenntartási folyamat esetén az alkatrészeket meghatározott fenntartási időközökben ellenőrzik, az esetleges veszélytelen meghibá-

sodásokat felismerik és a meghibásodott alkatrészeket újjal cserélik. Ebben az esetben a közelítő módszer alkalmazhatóságának feltétele, hogy a hibafelismerés és hibaelhárítás idejéből összetevődő karbantartási időtartam lényegesen kisebb legyen, mint a karbantartási ciklusidő.

Elektronikus biztonsági rendszerek esetén a fenti feltételek általában teljesülnek, így a közelítő módszerek alkalmazhatók. A veszélyes meghibásodásokra vonatkozó meghibásodási függvényre a közelítés a következő alakú:

$$P_v(t) = \alpha \cdot \left(1 - e^{-\lambda' \cdot t}\right) \tag{8-3}$$

8.2.3.2. A biztonsági számjellemzők és összefüggéseik

A fenti közelítések pontosságával a biztonsági számjellemzők a megbízhatósági jellemzők analógiájára képezhetők, a 8-2. táblázatban látható módon.

Megbízhatósági jellemző		Biztonsági jellemző	
Megbízhatósági függvény	R(t)	Biztonsági függvény	S(t)
Meghibásodási valószínűség	Q(t)	Veszélyeztetési valószínűség	G(t)
Meghibásodás sűrűség fgv.e	f(t)	Veszélyeztetés sűrűség fgv.e	g(t)
Meghibásodási ráta	λ(t)	Veszélyeztetési ráta	ρ(t)
Javítási ráta	μ(t)	Biztonság helyreállítási ráta	ν(t)
Üzemkészség	V(t)	Védelem jósága	Vs(t)

8-2. táblázat: Megbízhatóság és biztonság számjellemzői

A biztonsági jellemzők közötti matematikai összefüggések szintén hasonlóak a megbízhatósági jellemzőkkel kapcsolatban ismertetettekkel.
A biztonsági függvény:

$$S(t) = e^{-\int_0^t \rho(\tau)d\tau} \tag{8-4}$$

A veszélyeztetési függvény:

$$G(t) = 1 - S(t) = 1 - e^{-\int_0^t \rho(\tau)d\tau} \tag{8-5}$$

A veszélyeztetés sűrűségfüggvénye:

$$g(t) = \rho(t) \cdot e^{-\int_0^t \rho(\tau)\cdot d\tau} = \frac{dS}{dt} = \frac{dG}{dt} \qquad (8\text{-}6)$$

A veszélyeztetési ráta:

$$\rho(t) = \frac{g(t)}{\int_t^\infty g(\tau)d\tau} = -\frac{1}{S(t)} \cdot \frac{dS}{dt} = \frac{1}{1-G(t)} \cdot \frac{dG}{dt} \qquad (8\text{-}7)$$

A védelem jósága:

$$V_s(t) = \sum_i P_i(t) = 1 - P\{x_v(t) = 1\} \qquad (8\text{-}8)$$

A védelem jóságának (V_s) határértéke:

$$V_S(t \to \infty) = \frac{\nu}{\rho + \nu} = \frac{MTBD}{MTBD + MTTSR} \qquad (8\text{-}9)$$

ahol

- **MTBD** – (= **M**ean **T**ime **B**etween **D**anger) - a veszélyes hiba bekövetkezéséig tartó átlagos idő,
- **MTTSR** – (= **M**ean **T**ime **T**o **S**afety **R**epair) a veszélyes hiba átlagos javítási ideje.
- ν – a biztonság-helyreállítási ráta,
- ρ – a veszélyeztetési ráta

A meghibásodási ráta értéke az 1. fejezetben mondottak szerint a meghibásodás sebességére jellemző számérték. Ha különböző szempontok szerint a meghibásodásokat külön vizsgáljuk, akkor az egyes hibaosztályokra külön is meghatározhatók ilyen sebesség-paraméterek. Ezeket az adott hibaosztályra érvényes parciális meghibásodási rátának nevezzük. A biztonsági rendszerek különböző meghibásodási lehetőségei szerint vett parciális meghibásodási ráta értékek a 8-3 táblázatban láthatók:

A teljes rendszerre vonatkozó meghibásodási ráta a parciális meghibásodási ráták összegeként adódik:

Meghibásodás	Felismerhető	Fel nem ismerhető
Nem veszélyes	λ_{11}	λ_{12}
Veszélyes	$\lambda_{21}(\equiv \rho_{21})$	$\lambda_{22}(\equiv \rho_{22})$

8-3. táblázat: Parciális meghibásodási ráta értékek

$$\lambda = \lambda_{11} + \lambda_{12} + \lambda_{21} + \lambda_{22} \tag{8-10}$$

Fail-safe a rendszer, ha $\lambda_{22}=0$, biztonsági rendszereknél fontos, hogy λ_{12} értéke kicsi legyen. A fel nem ismerhető nem veszélyes hiba ugyan közvetlenül nem okoz problémát, de nagy értéke növeli a kettős hiba valószínűségét – és ez már veszélyes lehet!

8.3. A biztonság kockázat-alapú definíciója

8.3.1. A kockázat definíciója

A biztonság definíciójának másik lehetséges kiindulási pontja a kockázat lehet, amely ismét a 8-1. ábra szerinti eseménylánc alapján egy kárhoz vezető esemény fellépésének gyakorisága és az esemény során bekövetkező kár nagysága alapján határozható meg.

A kockázat már rendkívül régen kísérője az emberi életnek. Maga a szó a görög „rhiza" szóból származik, aminek jelentése „zátony": a nyereség vagy veszteség lehetőségét tartalmazza. A görög hajósoknak megvolt a reményük, hogy a partközeli utakon hajójukat baj nélkül célhoz juttatják, de annak a lehetősége is fennállt, hogy zátonyra futva hajójuk összetörik. A mai kornak is megvannak a kockázati tényezői (géntechnika, atomerőművek, közlekedés, rák stb.). A technika mindig kettős szerepet játszott, egyrészt segített a veszélyeket kizárni, ugyanakkor újabb veszélyeket hozott magával.

A kockázat definíciójának különböző lehetőségei:

- nyerés vagy veszteség lehetősége,
- a terv és a valóság közötti előre nem látható eltérés,
- kedvezőtlen események bekövetkezésének valószínűsége.

Kicsit álfogóbban mondható, hogy a kockázat annak a várakozásnak mértéke, hogy a természetes eseményekből, vagy emberi cselekvésekből, illetve mulasztásokból a civilizációban káros hatások keletkezhetnek az em-

berre, azok életfeltételeire, vagy környezetére. Eléggé elterjedt a kockázatnak mint biztosítási szakkifejezésnek a használata, amit egy kiváltó esemény és a vele kapcsolatban bekövetkező kár valószínűsége alapján határoznak meg.

A kockázat számszerűsíthető is: ebben az esetben a szokásos definíció szerint a kockázat a kár nagyságából (K) és bekövetkezésének valószínűségéből (p_E) képzett szorzat:

$$R = p_E \cdot K \tag{8-11}$$

A kockázat mindig valamely alapsokaságra vonatkozóan határozható meg. Ennek függvényében a kockázat lehetséges értelmezési módjai:

- *Egyéni kockázat*: annak a valószínűsége, hogy egy személy meghatározott esemény miatt előre meghatározott károsodást szenved (például gépkocsivezető halálos balesete). Ebben az esetben a kár nagyságát a károsodottak abszolút számával adjuk meg.
- *Kollektív kockázat*: fenti valószínűség személyek meghatározott csoportjára vonatkozóan. Ekkor a kár nagyságát a károsodottaknak az alapsokaságra vonatkozó relatív számával adjuk meg

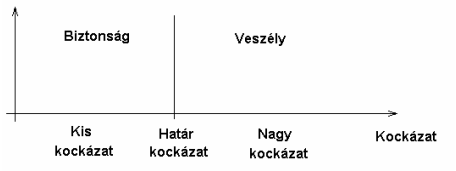
Bár a kockázattal kapcsolatban már valószínűségről beszélünk, s a kiszámítás módjára egy matematikai összefüggést alkalmazunk, mégis csupán minőségi definícióról van szó, melynél nyitva marad a kérdés, hogy az esemény gyakorisága és a kár nagysága között milyen funkcionális kapcsolat áll fenn.

A biztonság kockázattal kapcsolatos definíciójához az ún. határkockázati szint alapján juthatunk el, amely egy meghatározott műszaki folyamat vagy állapot legnagyobb, még elfogadható kockázatát jelenti.

Ennél a definíciónál abból indulunk ki, hogy akkor beszélhetünk biztonságról, ha a kockázat még elviselhető, vagyis egy határkockázati szint alatt van (8-3. ábra). Ez a határ általában mennyiségileg nem adható meg, hanem csupán minőségileg írható le. Ezzel egyidejűleg azt is kimondjuk, hogy ha biztonságról beszélünk, akkor egy meghatározott kis kockázatot azért feltételezünk.

A fenti definíció alapján megállapítható, hogy a teljes veszélytelenség értelmében abszolút biztonság nem létezik. Minden műszaki rendszer, minden léthelyzet tartalmaz bizonyos kockázatot. A biztonságtechnika feladata e kockázat csökkentése, bizonyos szint alatt tartása. A kockázat határértéke minden esetre nehezen határozható meg számszerűen, az a

technika fejlettségétől és társadalmi elképzelésektől függően határozható meg. Nem utolsó sorban azonban a mérnökök belátásától, felelősségétől függ, az optimális megoldás keresése, megtalálása fontos mérnöketikai problémákat vet fel.



8-3. ábra: A biztonság értelmezése a kockázati szint alapján

A biztonság kockázat-alapú definíciójából következő tények:

- abszolút (100%-os azaz teljesen kockázatmentes) biztonság nem érhető el!
- valamely műszaki rendszernél a szükséges biztonsági szint függ az emberek kockázattűrésétől,
- a megfelelő biztonsági szint mindig csak meghatározott környezeti feltételek között érhető el:
  - hőmérséklet,
  - nedvességtartalom,
  - mechanikus rezgés,
  - elektromágneses mezők stb.

A biztonsági rendszereknél a megfelelő műszaki kialakításon túl fontos, hogy a rendszer kezelése, fenntartása kifogástalan legyen. A kezelési hibák elleni védelmet garantálja a robusztus kialakítás (lásd a determinisztikus jellemzőknél a 3.2.1. fejezetben), védelem a véletlen és szándékos kezelési hibák ellen

8.3.2. Kockázat-elemzés

A biztonságkritikus rendszerek kialakítása során fontos feladat a biztonsági követelmények meghatározása. A biztonsági követelmények két területet ölelnek fel. Egyrészt meg kell adni a biztonsági rendszerrel szemben támasztott funkcionális elvárásokat, vagyis mindazokat a vezérlési és visszajelentési feladatokat, amit a rendszernek meg kell valósítania. Ezzel garantálható, hogy a hibamentesen működő rendszerben nem alakulnak ki

veszélyes üzemállapotok. Másrészt meg kell szabni a biztonság szintjére vonatkozó azokat a követelményeket is, amelyekkel garantálható, hogy a rendszerben jelentkező hibák, meghibásodások ne vezessenek veszélyes következményekhez. Ezek az ún. integritási követelmények írják elő a biztonság olyan mértékét, amelyekkel a funkcionális követelmények teljesíthetők. A biztonság ilyen mértéke a véletlenszerű meghibásodásokkal kapcsolatban általában számszerűen meghatározható, az ember által elkövethető szisztematikus hibákkal kapcsolatban azonban inkább csak minőségi kategóriák előírására van lehetőség. A biztonság-integritás szükséges mértéke csak akkor érhető el, ha a műszaki meghibásodások és szisztematikus hibák ellen hozott biztonsági intézkedések egymással összhangban vannak.

A kockázat minőségi értékelése a kár nagyságának és bekövetkezési valószínűségének (gyakoriságának) kategorizálásával lehetséges. Az irodalomban a következő lehetséges kockázati kategóriák szerepelnek (ezeket használják a vonatkozó szabványok is):

- R1 – elhanyagolható kockázat
- R2 – elfogadható kockázat
- R3 – nem kívánatos kockázat
- R4 – elfogadhatatlan kockázat

A kockázati kategóriák a két befolyásoló tényezőre vonatkozó kategóriák kombinációjaként határozhatók meg a következők szerint.

1. A kár nagyságára vonatkozóan négy lehetséges kategóriát határoztak meg. A legkisebb kármérték a jelentéktelen, utána a csekély, kritikus, végül a katasztrofális. Ezek nagysága a következők szerint írható le (lásd a 8-4. táblázatot):
2. A kár bekövetkezési valószínűségére 6 lehetséges kategóriát nevez meg a szabvány a legkisebb „hihetetlen”-ül ritka előfordulástól a „valószínűtlen”, „csekély”, „esetleges” és „valószínű” kategórián keresztül az állandó veszélyeztetést jelentő „gyakori” előfordulásig. Az egyes osztályok közelítő leírását és valószínűségére jellemző számértékeket a következőképpen szabhatjuk meg (lásd a 8-5. táblázatot):

Kár		Kockázati kategória	
jellege:	**nagysága:**	**neve:**	**jele:**
Haláleset	több	katasztrofális	4
	egy	kritikus	3
Súlyos sérülés	több		
	egy	csekély	2
Könnyű sérülés	több		
	egy	jelentéktelen	1

8-4. táblázat: Kár nagyságának lehetséges kategóriái:

Gyakorisági szint			
jele	**neve**	**leírása**	**nagyság [1/ó]**
A	gyakori	állandó veszélyeztetés	$> 10^{-3}$
B	valószínű	gyakori veszélyeztetés	$10^{-3} \dots 10^{-4}$
C	esetleges	többszöri veszélyeztetés	$10^{-4} \dots 10^{-5}$
D	csekély	legalább egyszeri veszélyeztetés	$10^{-5} \dots 10^{-7}$
E	valószínűtlen	veszélyeztetés kivételes esetben	$10^{-7} \dots 10^{-9}$
F	hihetetlen	veszélyeztetés nem várható	$< 10^{-9}$

8-5. táblázat: Bekövetkezési valószínűség kategóriái

A kárkihatás és az előfordulás gyakorisági kategóriáinak kombinálásával összesen 24 eset fordul elő, amelyet bizonyos a rendszerre vonatkozó megfontolások alapján besorolhatunk a kezdetben említett 4 kockázati kategóriába (8-6. táblázat

Valószínűségi szint	Kárkihatási kategóriák			
	Jelentéktelen	Cs ekély	Kritikus	Katasztrofális
Gyakori	R3	R4	R4	R4
Valószínű	R2	R3	R4	R4
Esetleges	R2	R3	R3	R4
Csekély	R1	R2	R3	R3
valószínűtlen	R1	R1	R2	R2
Hihetetlen	R1	R1	R1	R1

8-6. táblázat: Kockázati kategóriák

9. Biztonsági rendszerek

9.1. Műszaki folyamatok biztonsági tartalékállapottal vagy a nélkül

Az automatika rendszerek kialakítási módját elsősorban az határozza meg, hogy a kérdéses folyamat rendelkezik-e biztonságos tartalékállapottal, vagy sem. Biztonságosnak nevezzük azt az állapotot, amelyben az esetleg számításba vett meghibásodás ellenére sem jelentkezik veszélyeztetés. Bizonyos közlekedési eszközöknél például ilyen biztonságos tartalékállapot lehet az álló helyzet. A vonatoknál például alkalmaznak vészféket, amely segítségével ebbe a biztonságos állapotba lehet vinni a vonatot. Más példa lehet biztonságos állapottal rendelkező műszaki folyamatra egy atomerőmű, amelynél egy meghatározott üzemállapot esetén a reaktor kialakításától függő módon a folyamatot le lehet állítani és ezzel azt egy biztonságos állapotba lehet vinni. Mindkét említett példánál felismerhető, hogy a biztonságosnak definiált helyzet csak bizonyos körülmények között jelent valóban biztonságos állapotot. Például egy vonat álló helyzete nem tekinthető teljesen biztonságosnak, ha például éppen egy hosszú alagútban tartózkodik. Ugyanis ha a vonaton éppen tűz üt ki, akkor a vonat éppen a megállás miatt kerülne bizonytalan helyzetbe). Hasonlóképpen az atomerőmű példánál is azzal a feltételezéssel élünk, hogy a reaktor hűtőrendszere hibátlanul működik – csak ebben az esetben teremt biztonságos állapotot a vezérlő rudak reaktor térbe történő leeresztése.

A biztonságos tartalékállapot nélküli műszaki folyamatra példa lehet egy repülőgép repülése. Ezt a műszaki rendszert nem lehet leállítani bizonyos meghibásodások fellépése esetén (például a robotpilóta meghibásodása esetén). Kényszerleszállás is csak akkor lehetséges, ha a szükséges fedélzeti berendezések működőképesek.

A biztonságos tartalékállapottal rendelkező műszaki folyamatok esetén az automatika úgy alakítható ki, hogy veszélyes hiba esetén a rendszert ebbe a biztonságos állapotba vigye át. Az ilyen állapottal nem rendelkező műszaki folyamatok esetén a biztonságot csak igen nagy megbízhatósággal lehet garantálni. Ezekben az esetekben követelmény, hogy hiba fellépése esetén is működőképes maradjon a rendszer („fail operational” vagy „fail-op” rendszernek nevezik). Amennyiben a rendszernél még azt is megkövetelik, hogy egy további hiba esetén is működőképes maradjon, akkor a „(fail op)^2” rendszer elnevezés is szokásos az irodalomban.

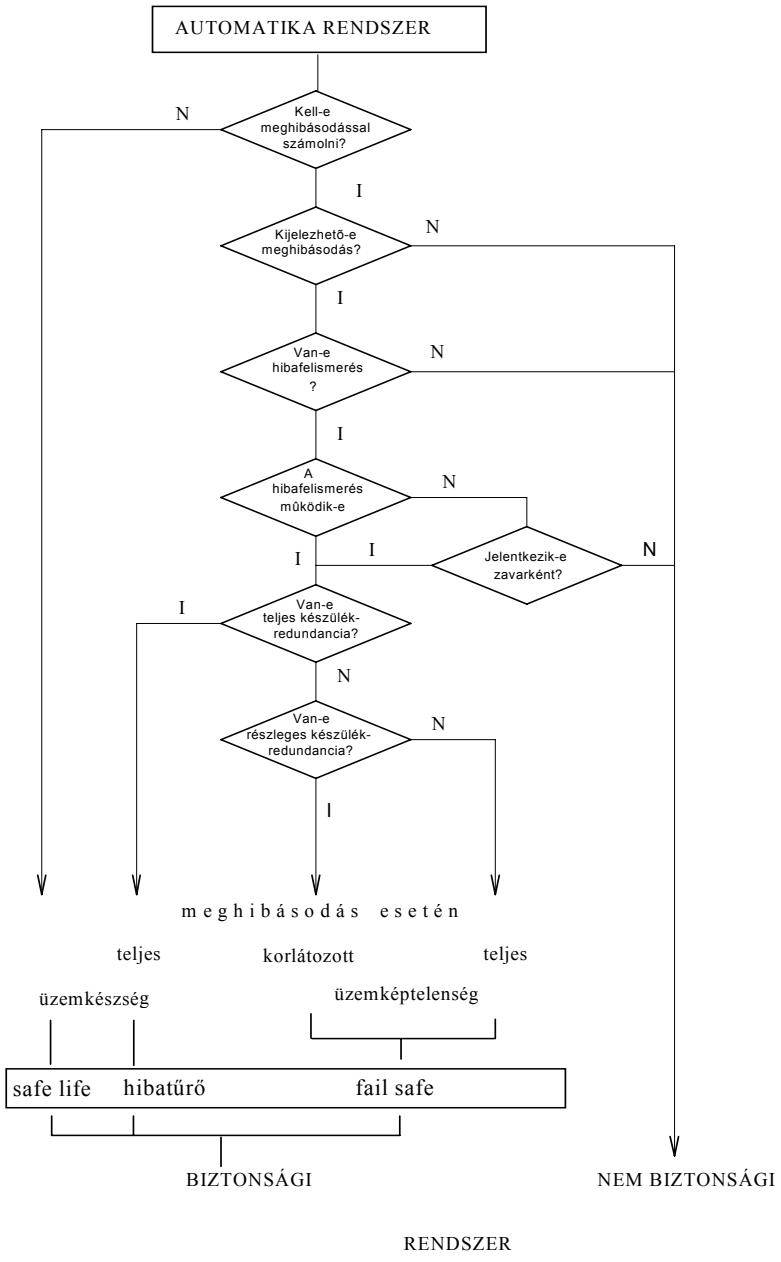
Egy adott pillanatban még hibátlanul működő folyamatvezérlő rendszernél felléphetnek olyan hibák, amelyek vagy veszélytelenek (például a készülék hőmérséklet-kijelzőjének meghibásodása), vagy pedig az automatizálási feladat hibás végrehajtásához vezethetnek. A hibás automatizálási funkció esetenként egyáltalán nem hat a kiadandó vezérlő jelekre, de lehet, hogy hibás vezérlő jeleket okoz. Ez utóbbi esetben biztonságot érintő hibás működésről beszélünk. A vezérlő jelek jellegétől függően gyakran veszélyes folyamatállapot léphet fel. Például sorompóval biztosított útátjáró-fedező berendezésnél hibás vezérlő jel okozhatja azt, hogy vonat közeledése nélkül is lezáródik a sorompó. Ez egy veszélytelen folyamatállapot lenne. Ha azonban a hibás vezérlő jel hatására a közeledő vonat ellenére sem záródna le a sorompó, az már veszélyes folyamatállapothoz vezetne. Ez a veszélyes folyamatállapot esetenként következmények nélkül marad, azonban következménye lehet egy baleset bekövetkezése is. Az előbbi például szerint a lezáratlan sorompó nem vezet balesethez, ha ugyanakkor nem közeledik közúti gépjármű a sorompóhoz. Csak akkor lesz baleset a következmény, ha a vonat és a közúti jármű egy időben ér a lezáratlan sorompóhoz. Ha a baleset be is következik, a hatása még lehet csekély, de ez személyek sérüléséhez is vezethet. A fenti eseményfolyamatból biztonsági szempontból csak a potenciálisan veszélyes meghibásodások képezik a vizsgálat tárgyát.

A korszerű µP-os automatikák alkalmazása során általában nem adható meg, hogy mely hibák vagy meghibásodások hatása lehet veszélyes az adott folyamatra, így ezeknél általában minden lehetséges hibát vagy meghibásodást potenciálisan veszélyesnek és így a biztonság szempontjából figyelembe veendőnek tekintenek.

9.2. A biztonságkritikus rendszerekkel kapcsolatos alapfogalmak

Biztonságkritikus rendszer alatt értjük azokat a rendszereket, amelyeknél fontos szempont, hogy esetleges meghibásodások esetén se lépjen fel veszélyeztetés.

Ezeket a rendszereket a meghibásodásokkal szemben mutatott viselkedésük alapján lehet alapvetően kategorizálni. A következő ábra mutatja be a biztonsági automatika rendszerek lehetséges kialakítási változatait (9-1. ábra).



9-1. ábra: Biztonsági rendszerek fő kialakítási módjai

9.3. Biztonsági automatika rendszerek kialakítási módjai

A biztonsági rendszereket kezdetben a fail-safe technika (stratégia) szerint alakították ki, például a jelfogós vasúti biztosítóberendezések esetében. Ez a klasszikus biztonsági stratégia – a tisztán hardver megoldásokra jellemző eljárás, aminek alkalmazását a fail-safe tulajdonságokkal rendelkező jelfogó, mint biztonságos áramköri elem léte tette lehetővé.

A mikroprocesszoros biztonsági rendszerek kialakítására alkalmazott stratégiák és eljárások:

- hibamentesség stratégiája: igyekszik a rendszerben előforduló hibákat elkerülni,
- hibatűrő stratégia: az el nem kerülhető hibákat fel kell ismerni és ezután hatástalanítani vagy hatását veszélytelenné kell tenni.

A hibamentes rendszerek fejlesztése terén a program igazolás elmélete már igen jelentős, a gyakorlati alkalmazást azonban a program konstrukció terén jelentkező nagymértékű kötöttségek akadályozzák. A biztonságigazolás a feladatok formális specifikációját igényli. Komoly leíró és specifikációs módszereket fejlesztettek ki, amelyekkel a formális specifikáció megoldható. A feladatkitűzés teljességét, konzisztenciáját vizsgálni kell, s a specifikációnak igazolható programra átírhatónak kell lennie. Még jelentős hiányok vannak az érvényesség-igazolás, a környezeti hatások feltételezett hatásának felmérése terén.

A hibatűrő stratégia terén egy sor elméleti eredmény és viszonylag kevés gyakorlati tapasztalat áll rendelkezésre. A leginkább sikert ígérő módszereket a megbízható rendszerek területéről vették át, illetve adaptálták.

A biztonságkritikus rendszerek életciklusa is az általános elveknek megfelelően a következő fázisokra osztható:

- rendszer-specifikáció – a funkcionális és biztonsági követelmények tisztázása
- követelmény-specifikáció – a funkcionális követelmények összeállítása,
- veszélyeztetések, kockázatok elemzése – a biztonsági követelmények összeállítása,
- a rendszer tervezése
- architekturális tervezés – a hardver és szoftver megosztása, a feladatok hozzárendelésével (hardver-szoftver „co-design”),

- hardver-tervezés és kivitelezés, tesztelés
- szoftver-tervezés és tesztelés
- teljes rendszer integrációja, a hardver és szoftver verifikációja („co-verification")

A rendszerek életciklusának kiinduló pontját jelentő rendszer-specifikáció bonyolult rendszerek esetén manapság csak terjedelmes verbális leírás formájában áll rendelkezésre. Az ilyen szóbeli megfogalmazású követelmény-rendszer mindig magában hordozza a nem-egyértelműség, a félreérthetőség kockázatát. Különösen akkor, hogyha külföldi gyártó esetén nyelvi értelmezési gondokkal is számolni kell a rendszer-specifikáció összeállítása során. Már ezen a szinten is nagy jelentősége lenne a verbális megfogalmazás mellett ún. szemi-formális vagy formális módszerek alkalmazásának.

Az életciklus következő fázisa a hazárdok, kockázatok elemzése, melynek során megállapítandók a lehetséges veszélyhelyzetek. A rendszer ilyen szempontból történő elemzésének a megbízhatóság-elméletben kialakult módszerei a **hibamód és hatás elemzés (FMEA)** valamint a **hibafa módszer (FTA).**

E két módszer elsősorban a vizsgálat irányát tekintve különbözik egymástól. Előbbi esetben a rendszert alkotó elemek (alkatrészek, részrendszerek) meghibásodásaiból indulunk ki és vizsgáljuk, hogy ennek milyen hatása lesz a teljes rendszerre vonatkozóan (induktív módszer). A másik módszer esetén pedig a rendszer lehetséges meghibásodásaiból indulunk ki és keressük, hogy milyen alkatrész-meghibásodás okozhatja ezt (deduktív módszer). Az elemzésekkel egyrészt a rendszer logikai viselkedését vizsgálhatjuk, másrészt az alkatrészekre vonatkozó megbízhatósági paraméterek (például meghibásodási ráta) ismeretében a rendszerre vonatkozó számjellemzők is meghatározhatók. E számjellemzők meghatározásának az elektronikus rendszerek terjedésével egyre nagyobb a jelentősége, hisz csak ezzel válhat összehasonlíthatóvá a régebbi rendszerekkel, illetve csak így lehetséges a rendszerek biztonsági szintjének számszerű meghatározása. Az elemzések alapján összeállítható a biztonsági követelmények dokumentációja. E két (a funkcionális- és biztonsági-) követelményrendszer adja a teljes rendszer-specifikációt. Ezután történhet meg a rendszer architektúrájának megtervezése, a hardver és szoftver közötti feladatmegosztás. E két rendszer-komponens tervezése korszerű megoldásban együttesen

végzendő („HW-SW co-design”). A tervezés eredményeként létrejön a hardver- és szoftver-implementáció a megfelelő dokumentációkkal.

Ezután következnek az életciklus igen fontos fázisai: a szoftver fejlesztés, az elkészített szoftver-modulok terve alapján azok integrációja, a megfelelő tesztlépésekkel. A biztonságkritikus rendszerek vizsgálatának két alapvető szintje a verifikáció és validáció.

A rendszer terve és a teljes rendszer-specifikáció alapján elvégezhető **verifikáció** során eldöntendő, hogy a rendszer megfelel-e a vele szemben támasztott követelményeknek, a fejlesztési folyamat elején meghatározott specifikációnak, vagyis funkcionálisan teljesíti-e az összes specifikációs előírást? A teljes rendszer **validáció**ja során a felhasználó ellenőrzi, hogy az elkészült rendszer valóban kielégíti-e az igényeit, tehát itt történik meg annak az ellenőrzése, hogy a specifikáció is a felhasználó igényeinek megfelelően történt. Ide értendő a biztonsági feltételek ellenőrzése, az ún. biztonságigazolás is. A megfelelőség ellenőrzése után megfelelő hatósági eljárás keretében történhet meg az ún. bizonylatolás (certification).

Mindezen fázisok után ér el az életciklus a rendszer használatának lehetőségéhez: megfelelő üzembehelyezési eljárás után kezdődik meg a rendszer üzemeltetése. Az életciklus fontos része a megfelelő karbantartás, amellyel a rendszer élettartama kedvezően megnövelhető.

9.4. A biztonságigazolással kapcsolatos kérdések

9.4.1. Általános megjegyzések

A biztonság értelmezési módja nem öncélúan, hanem mindig a műszaki fejlődésnek megfelelően módosul. A biztonságkritikus irányítástechnikai rendszerekben alkalmazott áramköri elemek meghibásodási jellegzetességei döntően befolyásolják azt. A korábban alkalmazott jelfogós rendszerek esetén bizonyos áramkör-kialakítási szabályok betartásával garantálható és ellenőrizhető volt a rendszer hibamentessége, az elektronikai, mikroelektronikai elemek használatával az értelmezés egyre inkább a kockázat alapú felfogás felé tolódik el. Ez alapvetően a biztonsági rendszerek kialakításának biztonságfilozófiáját is megszabja. Előbbi esetben egy ún. szabály-alapú biztonságfilozófia követése volt a jellemző, utóbbi esetben egyre inkább a kockázat-orientált gondolkodásmód a jellemző.

A biztonsági felelősséggel járó feladatokat ellátó automatika rendszerek általában csak akkor helyezhetők üzembe, ha azt egy műszaki felügyeleti hatóság engedélyezte. Ehhez biztonságigazolást kell végrehajtani,

amely alatt egy olyan dokumentációt értünk, amelyben ellenőrizhető módon szerepel, hogy az előírt biztonsági feltételeket a rendszer teljesíti-e.

Normál esetben ezzel a biztonságigazolással igazolja a folyamatautomatizálási rendszer tervezője a felügyeleti hatóság, illetve az üzemeltető felé, hogy a rendszer fejlesztése és gyártása során az érvényes szabványokat, előírásokat és követelményeket betartotta. Ennek során a biztonságos állapottal rendelkező műszaki folyamatoknál igazolják, hogy ezt a biztonságos állapotot a rendszer minden megkövetelt feltétel esetén eléri. Az engedélyezési eljárás során a biztonságigazolást a felügyeleti hatóság felülvizsgálja.

Az olyan folyamatautomatizálási rendszerek esetén, amelyek üzeméhez nem szükséges engedélyezési eljárás, a szerződő felek (a gyártó és üzemeltető) gyakran olyan biztonsági nyilatkozatot tesz, amely rögzíti, hogy milyen biztonsági előírásokat teljesít a rendszer.

9.4.2. Hibafilozófiai alapkérdések

9.4.2.1. Általános megjegyzések

A számítógépes biztonsági rendszerek fejlesztésének minden fázisában rendkívül fontos a hibaorientált gondolkodás. Egységes biztonsági gondolkodásmód szükséges a szoftverek fejlesztése során is. A szoftver vizsgálat és annak minőségbiztosítása még ma sem kellően megoldott problémák. A hardver és szoftver vizsgálatát általában nem lehet különállóan végezni, a kettőt együtt lehet csak kezelni.

A hibákat a korábbiak szerint a folyamatra gyakorolt hatásuk alapján lehet megítélni. Ilyen módon alapvetően megkülönböztethetünk veszélyes és veszélytelen hibákat.

A veszélyes hibák közvetlenül az emberek és gépek veszélyeztetését eredményezik. Ezek a hibák aktív hatást fejtenek ki a teljes rendszerre. Ezek megakadályozását feltétlen elsődleges célnak kell tekintenünk. A veszélytelen hibák önmagukban nem okoznak veszélyeztetést.

Ha a hiba semmilyen felismerhető hatást nem fejt ki a rendszerre, akkor passzív hibáról beszélhetünk. A passzív hibák más szintén veszélytelen passzív hibákkal kombinálódva már balesetveszélyes helyzethez vezethetnek.

A különböző szabványok, biztonsági előírások közötti lényeges eltérés az egyébként veszélytelen hibák figyelembe veendő kombinációinak mélységében van.

A rendszerek biztonsági vizsgálata során három hibamechanizmusból indulhatunk ki, amelyek a rendszer komplexitásától és az alkalmazási feltételektől függően különböző valószínűséggel léphetnek fel. Itt is előfordulhatnak

- szisztematikus hibák
- meghibásodások
- zavarok.

A tervezés, kivitelezés során szisztematikus hibák kerülhetnek a berendezésbe (hardverbe és szoftverbe egyaránt), amelyeket biztonsági rendszerek esetén feltétlenül fel kell ismerni és el kell hárítani az üzembe helyezés előtt, mert különben ezek mint fel nem ismert hibák egy előre meg nem határozható időpontban veszélyes állapothoz vezethetnek. A meghibásodás egy tulajdonság tartós megváltozása, ami üzembe helyezés előtt és üzem közben egyaránt jelentkezhet. E definíció alapján szoftverek esetén meghibásodásról nem beszélhetünk. A zavarok egy vagy több tulajdonság rövid ideig tartó megváltozásai.

A folyamatból adódó veszélyeztetés objektív és szubjektív megítélését a hibaszemléleti mód fejezi ki, melynél fontos befolyásoló tényező a figyelembe veendő hibák száma. A klasszikus egy-hiba szemlélet azt a követelményt jelenti, hogy egyetlen hiba nem vezethet veszélyeztetéshez. A hibák szekvenciálisan hatnak a vizsgálandó rendszerre, melynek során egy egyszeres hibát kell tekintetbe venni, az esetleges következményes hibákkal együtt. Független hibák kombinációja csak akkor jelentkezik, ha egy hibát nem ismertünk fel. A hibafelismerés és a hibára való reagálás módját a biztonságigazolás során kell vizsgálni.

A szabványok (melyek száma biztonsági feladatok vonatkozásában nem túl nagy, csupán néhány speciális területre vonatkozóan vannak ilyenek érvényben) részletesen foglalkoznak a folyamatok és azok automatizálásának szubjektív és objektív veszélyességével. Ezek mellett a biztonságtechnikai időértékek szinte háttérbe szorulnak. Márpedig a biztonság csak akkor garantálható, ha a hibákat megfelelő időben felismerve arra kellő időben reagál a rendszer. Mivel ezek az idők csupán a folyamat lefolyásától függenek, ezért ezeknek a veszélypotenciállal azonos módon nagy befolyásuk van a rendszertervezésre.

A figyelembe veendő fő időértékek a következők:

- a **hibatolerancia idő** az az időtartomány, amely alatt a rendszerben nem következik be veszélyes állapot a vezérlő- és szabályozó jelek meghibásodása esetén,
- a **reakcióidő** a hiba esetén az az időtartam, amely a hiba fellépésétől eltelik addig, amíg a rendszer eléri a biztonságos állapotát. Ez a reakció idő a hibafelismerési időből és a rekonfigurációhoz, illetve a lekapcsoláshoz szükséges időből tevődik össze. Az alapvető időfeltétel, hogy a hibareakció-idő kisebb legyen mint a toleranciaidő,
- a **második hiba bekövetkezési idő** az az időtartam, amelynek elteltével egy független második hibával kell számolnunk. Ez a rendszerre megállapított idő, amely függ a folyamat objektív veszélyességétől, a rendszer objektív megbízhatóságától, a rendszer objektív komplexitásától és szubjektív biztonságigényétől.

9.4.2.2. Alkatrészek meghibásodása és a biztonság

Az elektronikus biztonsági rendszerek biztonságigazolására vonatkozóan többféle előírás létezik, de ezekben vannak bizonyos közös vonások. Ilyenek a következők:

- egyszeres hiba esetén az elektronikus rendszernek úgy kell reagálnia, hogy a vezérelt folyamat ne kerülhessen veszélyes állapotba,
- megkövetelik, hogy az ilyen hibákat vagy hamar fel lehessen ismerni (és biztonsági intézkedéseket lehessen foganatosítani), vagy önműködően egy biztonságos állapotra vezessenek (amit a rendszer megőriz).
- ha az egyszeres hibák felismeretlenül maradnak, akkor a hibák vizsgálatát azok egy láncolatára ki kell terjeszteni,
- meg kell adni azokat a hibafajtákat, amelyekkel nem kell számolni.

Ezek a követelmények a veszélypotenciál mértékétől függően különböző erősségűek az egyes alkalmazási esetekben. Jóllehet a biztonság bináris mennyiség és a minőségi biztonsági vizsgálatoknál csak a követelmények teljesülését vagy nem teljesülését lehet megállapítani, közbenső állapot nem képzelhető el, mégis a különböző berendezésekre, alkalmazási területekre vonatkozó előírások különbözők lehetnek. Ilyen különbözőség lehet például abban, hogy a fel nem ismert hiba után a további hibák figyelembevételét milyen módon írják elő az utasítások. A vasúti berendezésekre vonatkozó előírások a kétszeres hiba felismerését, valamint a hibaszemlélet három hibára való kiterjesztését általában nem írják elő.

A biztonság ilyen különböző értelmezésének lehetősége magában a definícióban rejlik, miszerint „A biztonság az a képessége valamely vizsgált egységnek, hogy adott feltételek között és adott időn belül nem okoz veszélyeztetést” – itt az „adott feltétel”-eket lehet különbözőképpen értelmezni és ily módon lesz a biztonság értelmezése is bizonyos mértékig eltérő.

Ebből következik, hogy abszolút biztonság nincs, azt mindig viszonylagosan kell értelmezni. Valamely berendezést akkor tekinthetünk biztonságosnak, hogyha az adott esetre vonatkozó biztonsági követelményeket teljesíti. Egy biztonságos berendezés is meghibásodhat veszélyes módon, ha

- olyan hibák lépnek fel, amelyekkel egyáltalán nem számoltunk,
- olyan hibák lépnek fel, amelyeknek kizárása kellően megalapozottnak tűnt,
- olyan hibák lépnek fel, amelyek a fejlesztés során még ismeretlenek voltak, vagy figyelembevételüket elmulasztották,
- ha további hibák jelentkezése miatt az első hiba miatt felvett biztonságos állapotot elhagyja a rendszer.

Ezért minden biztonsági vizsgálatnak fontos kiinduló pontja a figyelembe veendő hibák listájának pontos rögzítése, az ún. hibakatalógus összeállítása.

9.4.2.3. Alkatrészek hibakatalógusa

Elektronikus rendszerek biztonságigazolása során rendkívül fontos, hogy az alkalmazásra kerülő alkatrészek lehetséges meghibásodásait összefoglaló hibakatalógusok rendelkezésünkre álljanak.

A különböző biztonsági rendszerek számára elfogadott hibakatalógusok állnak rendelkezésre Például a vasutak számára a vasutak nemzetközi szervezete, az ORE 1988-ban állított össze ilyen katalógust. Ebben elsősorban a helyhez kötött berendezésekben alkalmazott alkatrészekre vonatkozóan állapították meg a hibafajtákat. A járműveken telepített berendezések számára esetenként külön kell meghatározni a figyelembe veendő hibákat – mivel ott a környezeti feltételek mások. A hibakatalógus felállítása során a következő feltételezésekkel éltek:

- a hibák elkerülésére a fenntartási módszerek szigorúan előírtak,
- az alkalmazott alkatrészeknek megfelelő minőségi követelményeknek kell eleget tenniük,
- a hibakatalógusok esetén gyakran bizonyos hibákat figyelmen kívül hagynak, amennyiben erre megfelelő konstrukciós intézkedések lehe-

tőséget nyújtanak. Ezt természetesen az áramkörök konstruktőreinek mindig figyelembe kell venni. Valamely hiba figyelembevételének szükségességét csak az alkatrész gyártójával történő konzultáció eredményeként lehet eldönteni (mert esetleg az alkatrész gyártástechnológiájának kérdéseit is számításba kell venni). Mindig törekedni kell a legkedvezőtlenebb hibaeset figyelembe vételére.

9.4.2.4. A hibakatalógus alkalmazásmódja

Az elektronikus áramkörök kifejlesztése során figyelembe kell venni az alkalmazandó alkatrészeknél előforduló lehetséges meghibásodásokat.

Minden meghibásodás általában kijelzendő, hogy a többszörös hibák előfordulását elkerülhessük. Ha valamely hiba nem jelezhető ki azonnal, akkor ezeket más hibákkal együttesen is meg kell vizsgálni. A biztonsági vizsgálat általában a következő feltételezéseken nyugszik:

- a lehetségesnek tartott hibákat azonosítani kell,
- a meghibásodásokat a lehető leghamarabb ki kell jelezni, azaz a hiba jelentkezésének és kijelzésének időpontja közötti idő rövid legyen,
- két független hiba nem léphet fel egyidejűleg (vagy legalábbis is egy rövid időn belül). Egy rövid időszakon belül két független hiba fellépésének valószínűsége elhanyagolható kicsiny kell legyen,
- a jelentős hibafelismerési idővel rendelkező független hibák hatását az összes egyéb hibával együtt is meg kell vizsgálni, a nem független hibák hatását a kombinációkban mint egyszeres hibát kell figyelembe venni.

A gyors hibafelismerés érdekében a következő módszereket lehet alkalmazni:

- dinamikus működésmód,
- olyan vizsgálati módszerek alkalmazása, amelyek viszonylag rövid idejű ciklikus hibaellenőrzést tesznek lehetővé,
- információredundancia alkalmazása, hozzácsatlakozó összehasonlítással.

A hibafelismerés különböző műszaki megoldásainak a biztonság szempontjából azonos eredményhez kell vezetni, ezek csupán abban a struktúra-szintben különböznek egymástól, amelyen a hibakijelzés megtörténik.

A legújabb hibakatalógusokban már szerepelnek a mikroprocesszorok, amelyeknél aligha lehet valamennyi előforduló hibát számításba venni. Ha valamennyi matematikailag előforduló hibát tekintünk, melynek során a

hibákat a kimenetek párjaira, majd hármas stb. csoportjaira vizsgáljuk, akkor már viszonylag kis kimenetszám esetén sem kaphatunk reálisan kiértékelhető információkat. Így a mikroprocesszorok biztonsági vizsgálata nem végezhető ugyanazokkal a módszerekkel, mint a diszkrét áramköri elemeké.

9.5. A szoftver megbízhatóság és biztonság kérdései

9.5.1. A programhiba kérdése

A szoftverek hibamentessége fontos követelmény, a programhibák jelentős része éppen a programok bonyolultságának következménye. A teljes hibamentesség komplex rendszereknél általában nem érhető el, a program megbízhatósággal és annak igazolásával szemben a következő követelmények támaszthatók:

a) a rendszer nem lehet a működési lánc leggyengébb eleme: a műszaki folyamatban szereplő készülékek és emberi kezelések vonatkozásában az irodalomban rendelkezésre állnak megbízhatósági adatok. Az emberi hiba valószínűsége ritkán van 10^{-4} alatt, sokszor ezt az értéket írják elő határértékként.

b) a programhiba miatt bekövetkező károknak messze kisebbeknek kell lenni a rendszer alkalmazása nélkül várhatóknál. A követelmény teljesítéséhez a programhiba által okozott kárra, a programhívások gyakoriságára és a feltételezett hiba valószínűségére alapozott kockázat elemzésére van szükség.

c) a szükséges megbízhatóság elérésére és igazolására szükséges költségeknek messze kisebbnek kell lenni a számítógépek alkalmazásából származó nyereségnél. E követelmény azt jelenti, hogy a szoftver-hiba valószínűségének kis értéken tartására, illetve nagyságának meghatározására fordított költségeknek gazdaságos határokon belül kell maradni.

9.5.2. A programozói hiba kérdése

A szoftverek hibára való érzékenységének megállapítására éppen a programok komplexitását jelző mérőszámokat dolgoztak ki. E komplexitási metrikák közül talán legismertebb az M.H. Helstead által kidolgozott rendszer. A programozói hibák mennyiségére általános tulajdonságokból célszerű következtetni. A Halstead által kidolgozott elmélet szerint a programban várható hibák száma (B):

$$B = \frac{(N_1 + N_2) \cdot ld(\eta_1 + \eta_2)}{3000}$$

ahol:

- ld jelenti a 2 alapú logaritmust ($ld \rightarrow \overset{2}{\log}$)
- η_1 – a programban alkalmazott műveletek, operátorok száma – mindegyiket egyszer számolva
  $\{\eta_1\}$ = {=,+,-,/, ... go to A, go to B, if, begin ... end}
- η_2 – a programban alkalmazott változók (operandusok) száma, mindegyiket egyszer számolva
  $\{\eta_2\}$ = {változó1, változó2, ... , tömb1, tömb2, ...}
- N_1 – a programban előforduló összes műveletek száma (mindegyiket annyiszor számolva, ahányszor fellép)
- N_2 – a programban előforduló összes változók száma (mindegyiket annyiszor számolva, ahányszor fellép)

NB: a 3000-es szám az ember rövididejű memória-tulajdonságaiból és az angol nyelv sajátosságaiból adódó empirikus állandó.

A fenti egyenlet intuitív módon az alábbi módon értelmezhető: az η jelenti azt a szókészletet, ami a programozás során rendelkezésünkre áll: ($\eta = \eta_1 + \eta_2$). A programozás során minden lépéssel kapcsolatban ki kell választani, hogy a probléma megoldásához mely változók és mely műveletek szükségesek. A bináris kiválasztási lépések száma minden választási folyamat esetén $ld\eta$. Az $N = N_1 + N_2$ pedig megadja a szükséges választási folyamatok számát.

A logaritmus értékek mutatják, hogy a 3000-es nevező mellett gyakorlatilag nincs nagy szerepe a logaritmus alapjának. Nyilvánvaló, hogy ilyen egyszerű képlet a bonyolult programozási tevékenységet nem jellemezheti találóan még akkor sem, ha csak annak hibavalószínűségét vizsgáljuk. Mégis a hibák elkerülésének jó módszerének tekinthető az N_1 és N_2 kis értéken tartása. Az η_1 és η_2 növekedésének csak kisebb jelentősége van.

Más szóval ez azt jelenti, hogy minél jobban illeszkedik a programnyelv a megoldandó problémához, annál kevesebb hiba várható. A szótár növekedése csak kis mértékben, a program hossza viszont jelentősen befolyásolja a hibák számát.

A programozás következő fontos kérdése, hogy **gépi kód vagy magas szintű programozási nyelv** alkalmazása-e a célszerűbb? A fenti képlet alapján egyértelmű a magas szintű nyelv előnye, mert ennél adott terjedelmű problémát tekintve a képletben szereplő mind a négy változó kisebb, mint gépi kód esetén.

A fenti egyszerű képlet ellen szól, hogy a programozás minőségét egy sor más paraméter is döntően befolyásolja:

- hogyan fejlesztették a programot?
- közbenső teszteket alkalmaztak-e?
- hogyan szerveződött a programozó csoport?
- milyen segédeszközöket használtak? stb.

9.5.3. Követelmények a programnyelvvel szemben

A nyelv problémaorientáltsága és elterjedése bizonyos ellentmondásban van egymással. Ritkán használt, kevéssé ismert nyelv hátrány a fordítóprogram és egyéb segédeszközök vonatkozásában, ugyanakkor a fejlesztők és szakértők számára is kedvezőtlen. Másik oldalról minél inkább problémaközeli a nyelv, annál kevésbé ismert általános körökben, de annál inkább alkalmas a funkciók egyszerű megvalósítására.

A két ellentétes szempont között kell a megfelelő kompromisszumot megtalálni. A számítógépek egyre nagyobb elterjedtsége és a fordítóprogramok fejlődése miatt a jövőben a problémaorientált nyelvek szerepének növekedésére lehet számítani, amelyek az egyenlet szerint lehetővé teszik, hogy minimális N_i-vel és η_i-vel meg lehessen oldani a problémát.

A legfontosabb követelménynek mondható, hogy a programnyelv szintaxisa és szemantikája teljes és egyértelmű legyen. Ez elsősorban a programok áttelepíthetősége és a forrásprogram szinten tulajdonságaik igazolása szempontjából fontos.

Biztonsági feladat megoldására alkalmazott programnyelvnek segítenie kell a téves konstrukciók elkerülését, biztosítania kell az áttekinthető programkonstrukciót. Ebből adódnak a fontosabb követelmények.

a) Modularitás – a forrásprogramok áttekinthetőségére
   - o a nyelv segítse a modularizálást
   - o modulba való beugrás nem megengedett, kiugrás csak a modul végén, kivéve a hibakimenetet,
   - o a modulok 50–100 utasításból álljanak: a Halstead-összefüggés szerint ez még hibátlan lehet.

b) Eljárások lehetőleg rövidek legyenek
- a függvények nem változtathatják meg a paramétereket,
- hívás esetén ne keveredjenek össze a név- és értékparaméterek,
- max. 5 paraméter legyen,
- minden eljárásnak ellenőriznie kell, hogy a hívás jogos helyről történt-e és a hívásnál alkalmazott paraméterek megengedettek-e?
- Az eljárások hívásában nem szerepelhetnek más eljárások v. függvények.

c) Idő és sorrend problémák: A programellenőrzés megkönnyítésére
- a közös eszközöket szinkronizálni kell,
- az utasítás végrehajtása alatt az eszközöket nem szabad kívülről változtatni,
- megszakítás előre megoldott biztonsági programrészek futása alatt tilos,
- a leghosszabb megszakítás tiltás idejét előre meg kell adni,
- a program futásidejét könnyen ellenőrizni lehessen.

d) Ugrások, ciklusok, elágazások (csak a felhasználói programokra!)
- feltétlen ugrás előre nem megengedett
- cimke változók alkalmazása tilos
- a ciklusok ismétlődésének várható számát előre meg kell adni.

e) Adatok:
- implicit típus-konverzió ne legyen
- a változókat és tömböket típusokkal együtt határozottan deklarálni kell,
- a változónevek tetszőleges hosszúak legyenek,
- a változónevek segítsenek kifejezni, megadni, hogy a paraméterek
  - bemeneti, kimeneti vagy tranziens értéket reprezentálnak-e?
  - milyen fajtájúak (tömb, változó, konstans),
  - hol érvényesek,
  - mi a jelentésük?
- a változó rendszerparamétereket ki kell hangsúlyozni,
- a lokális és globális változók között különbséget kell tenni,
- egy adattípushoz egyetlen címzési technikát kell alkalmazni,
- a tömb méretek lehetőleg állandóak legyenek,
- a tömbelemek hívásakor valamennyi tömbdimenzió szerepeljen,
- a program futtatása alatt automatikusan ellenőrizni kell a határokat,
- EQUIVALENCE egyik fajtája se forduljon elő,

- egyszerű COMMON ne forduljon elő,
- az állandókat és a változókat egymástól elválasztva tároljuk (az ellenőrzés megkönnyítésére),
- a nem jogos felülírást automatikusan regisztrálni kell és meg kell akadályozni.

f) Programírás
- a program könnyű olvashatóságának előnyben kell lennie a könnyű megírással szemben,
- egy fajta írásnak mindig egy jelentése legyen és fordítva,
- a programban szabványos sorrendje és fix helye legyen a
  - megvalósítható/meg nem valósulható kódoknak,
  - deklarációknak,
  - inicializálásoknak,
  - formátumoknak,
  - kommentároknak.

g) Hibakezelés a program futtatása közben – automatikus hibajelzés szükséges
- tömbhatárok túllépése,
- értékhatárok túllépése,
- érték nélküli változók hívása,
- számértékek szignifikáns jegyeinek levágása,
- helytelen típusú paraméterek átadása esetén.

A fenti követelmények végül is redundanciának programba való beépítését célozzák a futás közbeni hihetőség vizsgálattal. E követelmények nem minden folyamatvezérlő számítógép alkalmazásánál ésszerűek. Részben bizonyos nyelveknél csak nagyon nagy ráfordítással lehet megvalósítani, részint azzal is megelégedhetünk, hogy a programozási előírásokban fektetjük le ezeket az elveket.

9.5.4. Követelmények a segédeszközökkel szemben

A program helyesség igazolása érdekében a programnyelvekhez hasonlóan a programozási segédeszközökkel szemben is támasztunk bizonyos követelményeket (fordító programok, könyvtári programok, futásidő és operációs rendszerek).

1. Általános követelmények
   - funkciójukat jól lássák el,
   - megbízhatóságukat kellő üzemi tapasztalat igazolja.

2. Követelmények a fordító programokkal szemben:
   - a fordítás alatt vagy után jól olvasható közbenső eredményeket kell kiadni,
   - a fordítási idő alatt a fordítóprogramon lehetőleg minél több ellenőrzést kell végrehajtani. Csak azokat az ellenőrzéseket kell a futásidő alatt végezni, melyeket korábban nem lehetséges (például paraméter típus vizsgálat),
   - a fordítás alatt talált hibákat csak kijelezni kell, javítani nem,
   - ha nem egyértelmű, hogy valamely szabályt nem tartották be, akkor figyelmeztető jelzést kell adni,
   - a fordítási idő alatt kell ellenőrizni minden szintaktikai konstrukciót, a változók értéktartományát, típusát, pontosságát, a hozzárendelések megengedhetőségét.

10. A minőség és a költség kapcsolata

10.1. Minőséggel kapcsolatos költségekről általában

A megbízhatóság növelésének triviális tényezői:

- megbízhatóbb alkatrészek alkalmazása,
- jobb minőségű gyártástechnológia,
- több mindenre kiterjedő, szigorúbb gyártásközi és végellenőrzés,
- tartalékolt struktúra (redundáns rendszer) alkalmazása,
- gondos üzemeltetés és karbantartás,
- szabályozott környezet, klíma.

A fentiek **mindegyikének jelentős gazdasági hatása van,** a termék árát, használatának költségeit emelik. Másrészt viszont a meghibásodások is okoznak költséget: javítás, pótlás, a folyamatok leállása miatti időkiesések, másodlagos károk stb. A kétféle költséget célszerű **együtt** vizsgálni, kiegészítve a termék használat utáni végső megsemmisítésének, anyaga újrahasznosításának kiadásaival, mivel ez utóbbi fajlagos értékét a termék élettartama befolyásolja. A minőségbiztosítás területén ezeket a költség-összetevőket az angol terminológia alapján a **COC** (**C**ost-**O**f-**C**onformance = a **„megfelelőség költsége”**) és **CONC** (**C**ost-**O**f-**N**on**C**onformance = a **„meg nem felelőség költsége”**) rövidítésekkel szokták jelölni.

A gazdasági optimum-keresés általában peremfeltételhez kötött szélsőérték számítás:

- vagy korlátozott költséggel kell maximális megbízhatóságra törekedni
- vagy korlátozott megbízhatatlanság mellett minimális költségre.

Az elemzés eredménye az, hogy a megbízhatóság növelése miatti költségnövekedés (a COC) a megbízhatósági szinttel progresszíven növekszik, a megbízhatóság csökkenése miatti költség (CONC) növekedése szintén progresszív jellegű. Az ismert módon két ilyen függvény szuperpozíciója egy határozott minimummal, azaz optimális megbízhatóságú ponttal rendelkező költség-függvényt eredményez. A gyakorlatban végül is legjobb esetben is csupán egy helyi optimumot lehet elérni, annak reményében, hogy az abszolút optimum (ha létezik) nincs nagyon távol attól.

Egyes különleges alkalmazásokban, ahol a biztonság növelése miatt adódó többlet költség gyakorlatilag nem számottevő az összes gazdasági

és egyéb hatásokhoz viszonyítva, **a méret, a tömeg is lehet korlátozó tényező** (például egyes űrkutatási, műholdon működő, orvosi, katonai berendezések). De akár egy autóban is egyidejűleg korlátoz a költség és a helyigény. (Két pótkerék nagyobb biztonságot adna mint egy, de három darab még nagyobbat. Még sincs értelme normális viszonyok között egynél több pótkereket hurcolni.)

Mindezeken túl a biztonság és a megbízhatóság nemcsak anyagi és mennyiségi vagy méretet érintő kérdés. Például katasztrófát okozhat, ha a repülőgép fedélzeti navigációs rendszere rossz döntést hoz. Az összes költség és méret mellett elhanyagolható többlet, ha megkettőzik a megfelelő processzorokat. Kérdés azonban, hogy ha landoláskor az egyik jobbra, a másik balra vezérelné a gépet, akkor mi történjék, hiszen az egyik hibás, de mi dönti el, hogy melyik. Felvetődik a gondolat: alkalmazzunk egy harmadik processzort, amelyik ilyenkor dönteni tud. De ha rendelkezésre állna egy ilyen okosabb harmadik, akkor minek kellett a másik kettő? Erre a problémára persze van megoldás, lásd a redundáns struktúráknál.

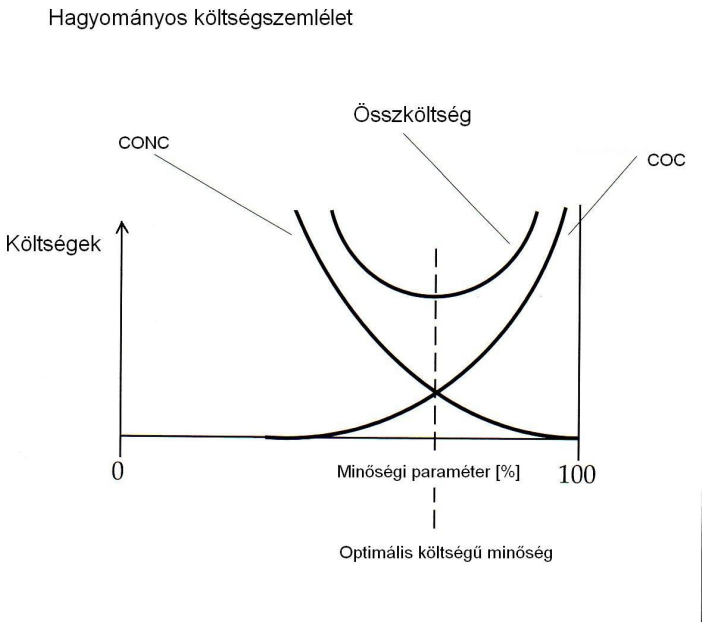
Összefoglalva:

A biztonság és a megbízhatóság minden határon túli növelése gyakorlatilag értelmetlen, a hibák előfordulásának teljes kizárása elvileg lehetetlen, viszont számos technológiai, rendszertechnikai lehetőség van arra, hogy az objektum gazdaságosan érje el

a **szükséges mértékű** megbízhatóságot**.**

10.2. A minőséggel kapcsolatos költségek különböző szemlélet-módjai

A minőség, az idő és a költségek olyan szoros kapcsolatban lévő három tényezőt jelentenek, amellyel kapcsolatban a szokásos gondolkodásmód szerint jobb minőséget csak nagyobb költséggel lehet elérni, illetve rövidebb átfutási idő feltétlenül a minőség romlásával jár együtt. A hagyományos szemlélet szerint az előző fejezetben említett két költségösszetevő figyelembevételével kellett (és lehetett) az optimumot megtalálni (10-1. ábra).



10-1. ábra: A minőség hagyományos költségszemlélete

A piaci versenynek jobban megfelelő gondolkodásmód szerint a három tényezőt – a minőséggel kapcsolatos költséget, a hibák miatt jelentkező kiadásokat és az időt - egyidejűleg kell csökkenteni.

Az üzemgazdasági költségszámítás mindig újabb utakat keres. Az eredeti költségszemléletben a COC és CONC keretében alapvetően három költségkomponens szerepelt, a megfelelősség költségösszetevőit a vizsgálati és hibaelhárítási költségek jelentették, míg a meg nem felelőséggel kapcsolatban a hibaköltségek jelentkeztek. A költségek újabb tagolása két csoportot állapít meg és így beszélhetünk a szerződésben foglaltakkal való egyezés illetve attól való eltérés költségéről. A megegyezés a cég sikeréhez való hozzájárulást, a meg nem egyezés pedig a felhasznált eszközök felesleges pazarlását jelenti. Ez a költségszemlélet sem teszi azonban lehetővé a teljes értékteremtési folyamat egészének ábrázolását. A közgazdasági, üzemgazdasági részleteket mellőzve megállapítható, hogy a minőség a versenyképesség egy döntő tényezője, ezért napjainkban és a jövőben egyre inkább nagy jelentősége lesz a cégek üzletvitelében.

10.3. A biztonsági rendszerekkel kapcsolatos költségek

10.3.1. Általános megjegyzések

A biztonság a korábbiak szerint úgy definiálható, mint az az állapot, amelyben nem következhet be természetes vagy jogi személyek javainak sérülése. A biztonság így leírt állapotában az embernek az élethez való ősi ragaszkodása tükröződik. De ennek az igénynek a teljesítése ellen hat a tökéletlenség, a mulandóság természettörvénye. Tehát a biztonságra, mint egy állandóan és örökké fenntartandó állapotra ugyan lehet törekedni, de azt maradéktalanul elérni nem lehet. Az általános nyelvhasználat mutatja azt a tényt, hogy az abszolút biztonság csak elméletileg képzelhető el, amennyiben a biztonságot az abszolút biztonság többé kevésbé jó közelítéseként fogjuk fel. A biztonságnak ez a viszonylagosként való természetes felfogása kényszerűen megköveteli a viszonylagosság leírását. Az ismertetett definíciós lánc alapelvéből először az a leírási mód adódna, hogy a biztonság az ideális állapottól a veszélyeztetések síkján való eltérés lenne. A veszélyeztetések azonban események, amelyek nagyon nehezen regisztrálhatók és valóban csak nagyon ritkán regisztrálják is ezeket, mert bekövetkezésük önmagában még nem alapoz meg valamilyen jogi következményt. Például a légi közlekedés esetén a légiforgalom-irányítók jegyzik a repülőgépek veszélyes találkozásait és ezeket évente a légi forgalom biztonsági mérőszámának tekintik, de az ezekben az eseményekben részes légi utasok legfeljebb csak saját tapasztalatuk alapján észlelik ezeket. Hasonló szituációk kezelése a közúti forgalomban már eleve lehetetlen a regisztráció az átfogó ellenőrzés hiánya miatt.

Egész más a helyzet, ha a veszélyeztetés miatt bekövetkezett baleset már kár formájában jelentkezik. A védett javak sérüléséből, különösen a tulajdonban és az egészségben, esetleg emberéletben okozott károk miatt mindig magánjellegű kártérítés, sőt esetenként nyilvános eljárás igénye jelentkezik, ami szükségessé teszi az esemény körülményeinek többékevésbé pontos felmérését. E kártérítési igények kielégítésén túl a regisztráció lehetővé teszi a veszélyeztetésekről gyakorisági, valószínűségi adatok gyűjtését is. A pótolhatatlan javak veszélyeztetése különösen fontos kategória a károk megállapításánál (egészség, emberéletben esett károk). Így a halálozási gyakoriság, illetve ~ valószínűség különösen fontos biztonsági számjellemző. Ezek a gyakoriságok mindig meghatározott eseményre vo-

natkoznak, egy adott időtartamon belül (például haláleset évente, Magyarország teljes népességére vonatkozóan).

Minél nagyobb a vizsgált kollektíva és időszak, annál inkább megengedhető, hogy a kapott számjellemzőket valószínűségi értékekként használjuk. Német viszonyokra statisztikai alapon meghatározott számértékek alapján a publikációkban óránkénti kb. 1:1.000.000 halálozási arány szerepel az általános betegségi okokra vonatkozóan. Matematikailag ez a következőképpen fejezhető ki:

$$w_A = 10^{-6} \left[\frac{\text{haláleset}}{\text{fő} \cdot \text{óra}} \right] \qquad (10\text{-}1)$$

Hasonló értékek szerepelnek az amerikai viszonyokra vonatkozóan is. Így ez a szám mint az élet alapkockázata vehető figyelembe, ilyen kockázatnak van kitéve minden ember, pusztán a léte alapján.

10.3.2. A társadalompszichológiai kockázattűrés

Az alapkockázat mellett még számos kockázati tényező szerepel, aminek nem teljesen azonos kényszerűséggel, de ki van téve az ember. Az ilyen kockázatok elviselése abból a tényből adódik, hogy a biztonság csak az egyik fontos elvárásunk az élettel szemben, ezt még egy sor más, az életminőséggel szembeni követelmény egészíti ki.

A biztonság aránya az életminőségen belül nyilván személyenként változó. Van, akinek az életveszély leküzdése különösen fontos életérzést jelent, mások minden kockázattól mentesen szeretnek élni.

Ezért óhatatlanul felmerül a kérdés, különösen a műszaki létesítményekkel, rendszerekkel kapcsolatban (amelyek részben kényelmesebbé, komfortosabbá teszik az életet, másrészt azonban jelentős veszélyeztetést vagy környezetkárosítást jelenthetnek): mekkora biztonság az „elegendő biztonság”?

Az egyik lehetséges válasz az lehet, hogy

elegendő a biztonság,
ha minden nemű veszélyeztetés kizárt.

Ismerve, hogy abszolút biztonság nem létezik, ez a válasz láthatóan nem eléggé gyakorlatias, a valóság tényeit nem veszi kellően figyelembe.

További válasz lehet, hogy

elegendő a biztonság,
ha mindent megtettünk a veszélyeztetések kizárására.

Ez a válasz már elismeri az abszolút biztonság elérésének lehetetlenségét és a biztonsági követelményt ésszerűen a reálisan megvalósíthatóhoz igazítja. De ha ez alapján kíséreljük meg a műszaki rendszerek esetén a szükséges biztonsági intézkedéseket kialakítani, akkor nagyon hamar megállapíthatjuk, hogy minden elért biztonsági szinthez további intelligencia és költség bevetésével mindig adódik egy növelési lehetőség. E növelés megvalósítása után ismét adódnak biztonságtechnikai lehetőségek a biztonsági szint növelésére, ha egyre újabb és nagyobb ráfordításokkal, úgyhogy végül be kell látni, hogy az „olyan biztos, amilyen csak lehet" irányelvvel kimondatlanul, de ismét az abszolút biztonságot követeljük meg. Ezért végül ezt a választ is irreálisnak és a gyakorlati biztonsági intézkedések számára alkalmatlannak kell minősítenünk.

A biztonságkritikus rendszerek (berendezések és szervezetek) eddigi fejlődésére tagadhatatlanul gyakran a műszakilag lehetséges biztonsági szint alapgondolata volt jellemző, s néha még ma is az. Az abszolút követelményt végül is a fenti okok miatt nem lehetett teljesíteni. Valamikor csak megszakadt a biztonsági szintek fokozatos növelésének folyamata, de nem egy objektív szint elérése miatt, hanem többé vagy kevésbé felismerhető módon, de szinte mindig az „ez a szint már igazán megfelelő" teljesen szubjektív becslés alapján. Ez a csak a műszakilag lehetséges szintre orientált biztonsági fejlesztés és a vele kapcsolatos költségek német vélemények szerint kockáztatják a vasutak versenyképességét.

Közvetve az eredeti kérdésünkre adott harmadik lehetséges válaszból adódott az igény arra, hogy egy lehetőség szerint objektív mértéket találjunk a biztonsági szintre. Ez a válasz:

elegendő a biztonság,
ha „mindent" megtettünk, amit „kell".

A „kell" szócskában felismerhető, hogy a szükséges biztonsági szint meghatározása nem kizárólag a biztonságtechnikusok ügye, hanem csakis a biztonságot kialakítók és a maradék kockázatot elviselők közötti kompromisszum eredménye lehet.

Ebben az értelemben vizsgálható, hogy a biztonsági szintet igénybevevők részéről milyen követelmények támaszthatók az elérendő biztonsági

szinttel szemben. Korábban megállapítottuk, hogy az az igény, hogy biztonságosan élhessünk, az egyéb életkövetelményekhez képest egyénenként nagyon különböző prioritású lehet. Most tehát azt kellene vizsgálni, hogy az egyének biztonságértékeléseinek statisztikai összegéből lehet-e törvényszerűséget megállapítani a megkövetelt biztonsági szintre vonatkozóan, vagyis azt a kérdést tehetjük fel:

„Mekkora az a kockázat, amit a társadalom elvisel és milyen tényezők befolyásolják ezt a kockázattűrést?"

A fenti kérdésre adott válasz alapja elsősorban nem műszaki/matematikai, hanem inkább pszichológiai jellegű. Ha tehát a problémát kissé tudományosabban akarjuk megfogalmazni, akkor azt kérdezhetjük, hogy:

Milyen törvényszerűségeket követ a társadalom-pszichológiai kockázattűrés?

Szokás a kérdés megválaszolásánál az élet alapkockázatából kiindulni és ehhez viszonyítva bizonyos különbségeket megállapítani a kockázattűrést illetően. A vizsgálatok első alapmegállapítása az, hogy az emberek általában magukban sokkal jobban megbíznak egy magasabb biztonsági szint elérését tekintve, mint másokban. Ebből indirekt módon az következik, hogy a tényleges kockázattűrés annál nagyobb, az elvárt biztonsági szint annál kisebb, minél inkább maga a felelős az ember a saját biztonságáért. És fordítva, a tényleges kockázattűrés annál kisebb, az elvárt biztonsági szint annál nagyobb, minél inkább más veszi át a felelősséget az ember biztonságáért. Ha tehát a saját és idegen felelősség arányát durván négy lehetséges osztályba soroljuk, akkor a következő kockázattűrési értékeket határozhatjuk meg:

- kizárólag saját felelősség: főleg a teljesítményjellegű sport tevékenységek során az élet alapkockázatának 100-szorosát is elfogadja az ember:

$$w_{\text{saját}} = 10^{2} \cdot w_{A} = 10^{-4} \left[\frac{\text{haláleset}}{\text{fő} \cdot \text{óra}} \right] \qquad (10\text{-}2)$$

- vegyes saját és idegen felelősség, de túlnyomóan saját felelősség esetén, a háztartásokban, a munkavégzés közben, illetve jellemző módon az egyéni közlekedés során, a kockázattűrés mértéke kb. megegyezik az élet alapkockázatával:

$$w_{\text{saját/idegen}} = w_A = 10^{-6} \left[\frac{\text{haláleset}}{\text{fő} \cdot \text{óra}} \right] \tag{10-3}$$

- ismét vegyes, de most túlnyomóan idegen felelősség (például a tömegközlekedés) esetén legalább egy nagyságrenddel kisebb a kockázattűrés, mint az élet alapkockázata:

$$w_{\text{idegen/saját}} = 10^{-1} \cdot w_A = 10^{-7} \left[\frac{\text{haláleset}}{\text{fő} \cdot \text{óra}} \right] \tag{10-4}$$

- kizárólag idegen felelősség (nagy ipari létesítmények közvetlen szomszédságában) esetén két nagyságrenddel is kisebb lehet a kockázattűrés, mint az élet alapkockázata:

$$w_{\text{idegen}} = 10^{-2} \cdot w_A = 10^{-8} \left[\frac{\text{haláleset}}{\text{fő} \cdot \text{óra}} \right] \tag{10-5}$$

A társadalompszichológiai kockázattűrés és az élet alapkockázatának viszonyában figyelembe kell venni azt a tényt, hogy az élet alapkockázata nem állandó érték, hanem országonként és időben változó nagyság. A múltban egy-egy országban az orvostudomány fejlődésével érte el mai szintjét és a jövőben is ennek függvényében fog változni.

A vasutak számára a fenti vizsgálatokból adódó fontos tény, hogy vele szemben a társadalomnak magasabb biztonsági elvárásai vannak, mint a közúti közlekedésnek. Ez objektíve egy versenytorzulást eredményez az azonos feladatot ellátó közlekedési ágak között. Azonban ezen a társadalompszichológiai tényen az ismételt és mégoly nyomatékos utalásokkal is alig lehet változtatni, jóllehet a vasutaktól kb. 10-szer nagyobb biztonságot követelnek, mégis a közúttal egyenértékűnek tekintik.

A vasutak az elért biztonsági szintet, ami messze teljesíti a társadalompszichológiailag elfogadott kockázattűrésnek megfelelő értéket, természetesen nem kívánják csökkenteni és a biztonsági intézkedéseket is a megkezdett irányban kívánják folytatni, mégis nagyon fontos, hogy ezt a fejlesztést ne véletlenszerűen, hanem objektív mértéket figyelembe véve végezzék.

10.3.3. A biztonság és a gazdaságosság

Az általános biztonság definíciójából az élet különböző területeire az ott mértékadó tulajdonviszonyok alapján határozhatók meg specifikus bizton-

sági fogalmak. Így például a vasútnak is, mint jogi személynek tiszteletben kell tartania azoknak a személyeknek a javait, akik vele kapcsolatba kerülnek. Ide tartoznak mindenek előtt a termelőrendszerben közreműködő személyek, akik, általánosan fogalmazva a biztonságos munkakörülményekre, vagyis munkabiztonságra tartanak igényt. Mindenek előtt azonban azoknak a személyeknek a javaira kell vigyáznia, akik magukat vagy tulajdonaikat a szállítás során a vasútra bízzák. Ekkor a vasútnak különösen a szállítási biztonságot kell garantálni. Harmadszor felelősséggel tartozik a vasút azoknak a személyeknek is, akik sem nem dolgoznak a vasútnál, sem nem veszik igénybe a vasút szolgáltatásait, hanem csupán ideiglenesen vagy tartósan fennálló szomszédviszonyban kerülnek kapcsolatba vele. A személyeknek ez a köre a környezetbiztonságra tart igényt. A munka-, szállítási- és környezetbiztonság három területén az igények semmiképpen nem egyoldalúak: ahogy a vasút a dolgozóit védi, fordítva igényt tart a dolgozói részéről is a védelemre. Hasonló igaz a szállítás és környezetbiztonság területén is.

A munka- és környezetbiztonság minden termelő rendszerben újra találkozik. A szállításbiztonság azonban a vasút szolgáltatási feladataiból, mint a vasútra jellemző specifikus feladatból vezethető le. Így ez szükségszerűen az egész vasúti szervezetet és forgalom-lebonyolítást olyan módon befolyásolja, ami más termelő ágazatoknál nem ismert. Ebből ismét következik, hogy a szállításbiztonság a vasút gazdaságosságát is alapvetően meghatározza.

Erős egyszerűsítéssel a vasút gazdaságosságának mérőszámául az üzemi bevételeknek az üzemi kiadásokhoz viszonyított nagyságát tekinthetjük. Vizsgálandó lenne, hogy e két tényezőt milyen módon befolyásolja a szállításbiztonság mértéke. A szállításbiztonság mértéke valamennyi kockázatra vonatkozóan az élet alapkockázatának megfelelő halálozási kockázat lehetne.

Közvetlenül belátható, hogy az egyre kisebb szállítási kockázat elérésére alkalmazott biztonsági ráfordítások elvileg növekednek, sőt progresszíven növekednek. A biztonsági ráfordítások részét képezik az üzemi kiadásoknak. Alapvetően tehát a növekvő biztonsági ráfordítások negatív hatást gyakorolnak a gazdaságosságra.

Az üzemi bevételekre érvényes lehetne, hogy első közelítésben azok mindaddig függetlenek az elért biztonsági szinttől, amíg a társadalompszichológiai kockázattűrés mértékét a maradék kockázat nem lépi túl. Csak

ezután jelentkezik az ügyfelek elvándorlása (elpártolása), ami a bevételeket csökkenti és így a gazdaságosságot ismét negatív módon befolyásolja.

Összességében általában megállapíthatjuk, hogy a szállításbiztonság érdekében tett biztonsági intézkedések gazdasági optimumot a társadalompszichológiai kockázattűrés közelében kell keresni.

Erre a gazdasági optimumra nemcsak belső üzemi okok miatt kell törekedni, hanem általában is helyes célkitűzésnek kell tekinteni, ha abból a gondolatból indulunk ki, hogy azok a gazdasági források, amelyekből a biztonsági ráfordítások kielégíthetők, nem korlátlanok. Azok a ráfordítások, amelyek egy speciális területen a biztonságnak messze a kockázattűrés által meghatározott szint fölé emelésére használnak fel, feltehetően jelentős biztonságnövekedéshez vezetnek. De az ezzel összefüggésben szintén progresszíven növekvő ráfordításokhoz nem állnak rendelkezésre megfelelő eszközök, hogy az élet alapkockázatát csökkentsük, vagy más, biztonságra érzékeny területen legalább az élet alapkockázatát elérjük. Például az útátjárók teljes kiküszöböléséhez és ezzel a velük kapcsolatos kockázat 0-ra csökkentéséhez szükséges nagy ráfordítások hiányozhatnának például a rákkutatásra szánt összegből és akadályoznák, hogy az élet alapkockázatát általánosabb jelleggel csökkenteni lehessen.

Bizonyára nem lehet itt szó a ráfordítás-biztonság viszonyának össztársadalmi szintű optimalizálásáról, az általános összefüggések vizsgálatának csupán az a célja, hogy a biztonsági mérnökök szemléletében olyan jellegű szemléletváltozást eredményezzen, hogy a ráfordításoknak, a gazdasági kérdéseknek a biztonsági területen való megemlítése nem feltétlenül jelenti az emberélet semmibevételét a maximális nyereség érdekében.

10.3.4. A kockázattűréshez való illesztés módszerei

A műszaki rendszerek biztonsági szintjének elfogadható szintre emelése olyan régi feladat, mint a műszaki fejlesztés maga. Különösen az ipar kezdeteinél oldották meg ezt a kérdést elvileg oly módon, hogy a konstrukciót lényegében a funkció alapján határozták meg és a biztonsági intézkedéseket csupán az üzemeltetés során bekövetkezett balesetek alapján határozták meg. Más vélemények szerint meg kell állapítani, hogy nemcsak maga a bekövetkezett baleseti esemény, hanem a társadalmi nyilvánosság megfelelő reakciója is a biztonsági intézkedések kiváltó tényezője lehet. Bizonyára nem lehet általában kijelenteni, hogy a kockázattűréshez való empirikus alkalmazkodás tudatosan és a „kezdeti veszteségek” cinikus számításba vételével történt, mivel maga a műszaki megoldás egyáltalán és

a hozzátartozó biztonsági intézkedések lehetőségei még messzemenően ismeretlenek voltak. Csak az egyre gyűlő tapasztalat teremtett meg egy bizonyos értelemben vett előretekintő biztonsági szemléletet és egy biztonsági intézkedés-katalógust, ami hasonló problémák megoldására a fejlesztések számára is rendelkezésre állt. Mindenképpen megállapítható, hogy végül is a biztonságtechnika még ma is főleg az empírián alapszik. Példaként emlékeztethetünk a repülőgépek anyagának tartós szilárdságára, amit csupán egy brit repülőgéptípus feltűnést keltő sorozatos balesete után ismertek fel. A közúti közlekedésnél alkalmazott passzív biztonság érdekében hozott intézkedéseknél különösen felismerhető a biztonsági intézkedések tapasztalat orientált jellege, amelyeket a balesetek bekövetkezése után az okok és következmények elemzése alapján vezettek be, jóllehet ezek hatékonysága önmagában már korábban is felismerhető lett volna.

A vasútnál alkalmazott biztonsági intézkedések széleskörű katalógusa szintén nem tagadhatja empirikus eredetét. A magyarázat érdekében kissé túlozva azt mondhatjuk, hogy a vasúti biztosítóberendezések története egyben a vasúti balesetek története is. A ma használatban lévő biztonsági berendezések számos eleme egyértelműen balesetre vezethető vissza. Meghatározott konstrukciós elvek figyelembevétele is – amelyek ma még mint absztrakt követelmények jelentkeznek, mint például az aggályosság elve, a védő visszautasítás elve – a balesetek elemzéséből került be a gyakorlatba. Azt gondolhatnánk, hogy éppen a vasutaknál, több mint 100 éves baleseti- és biztosítási történet után a biztonsági módszerek tovább fejlesztése inkább eltávolítható az empíriától, mint egyéb biztonságkritikus területeken.

Valójában meg lehet állapítani, hogy a látványos következményekkel járó balesetek még mindig igen erős impulzusokat jelentenek a biztonsági intézkedések számára – szinte függetlenül a velük kapcsolatos ráfordításoktól (például gondolhatunk a sebességellenőrző pontok utólagos kiegészítésére az 1971-es Aitrang-i baleset következtében, hasonlóan a kisforgalmú vonalak térközberendezéssel való felszerelésében nem kis szerepet játszottak a Warngau-i és Radeformwald-i balesetek). A balesetek után végrehajtott műszaki átalakításokkal vitathatatlanul kiküszöbölhetők lettek a hasonló esetek, de továbbra is megmaradt a kérdés, hogy a vele kapcsolatos biztonsági ráfordításokat ilyen látványos ösztönzések nélkül más területeken nem hatékonyabban lehetett volna-e felhasználni? A biztonsági eszközök biztonsági szint növelését célzó felhasználásának véletlenszerű szabályozása bizonyára nem tekinthető a költség-biztonság viszony

optimális összehangolásának. Az ember könnyen hiszi azt, hogy a valóban bekövetkezett dolgoknak nem lehet csekély eseményvalószínűsége. Amerikai irodalmi adatok alapján azonban megállapították, hogy az USA Atomerőművi Bizottsága (NCR) a Harrisburg melletti Three-Mile-Island atomerőmű zavarai után az esemény pszichológiai hatása alatt fordította figyelmét az e fajta zavarokra, jóllehet más jellegű zavarok objektíve legalább ilyen valószínűek voltak. (Hazai példa lehet a pörbölyi vasúti baleset, aminek pszichológiai hatása alatt történt meg a tartalék áramforrást jelentő akkumulátorok típusának cseréje stb.).

Összefoglalóan megállapíthatjuk, hogy a társadalompszichológiai kockázattűréshez való empirikus alkalmazkodás módszerének három hátránya is van:

- a műszaki rendszerek szükséges biztonsági szintje csak a baleseti következmények túlzott figyelembevételével érhető el,
- a biztonsági szemlélet alakítása a véletlen események által alkalmas arra, hogy a figyelmet az esetleg nagyobb veszélyforrásokról elterelje,
- a gazdasági erőforrások biztonság növelésére való felhasználásának a véletlen balesetektől függő felhasználása csak véletlen, de bizonyára nem optimális ráfordítás-eredmény viszony elérését teszi lehetővé.

Mindezekből következik, hogy már nagyon időszerű lenne legalább megkísérelni, hogy a társadalompszichológiai kockázattűrés figyelembevétele során az optimális ráfordítás-eredmény viszony elérésére szisztematikus-analitikus módszertant lehessen kialakítani.

A megoldás itt nyilván nem a szokásos költség-haszon összevetést alkalmazó értékelemzés alkalmazása lesz, ahol függetlenül attól, hogy hogyan határozhatjuk meg a haszon nagyságát, végül is a biztosítási matematika alapján az egészséget, emberéletet pénzráfordításokkal veszik figyelembe. A pótolhatatlan veszteségeket nem lehet pénzszerűen kifejezni. Másrészről ez a módszer is csak a tapasztalatokra alapoz, mivel bizonyos baleset típusokat úgy kell a rendszer üzeme során meghatározni, hogy elkerülésükre ezekkel egy megfelelő ráfordítást lehessen szembeállítani. Végül pedig a baleset, illetve annak következménye csak utolsó láncszem egy eseményláncban, úgyhogy a biztonságelemzésnek csupán a baleseti eseményekből való levezetését már ebből a tényből kifolyólag is tökéletlen módszernek kell minősítenünk.

11. Minőségbiztosítás

11.1. Alapfogalmak

11.1.1. Minőség

A minőség és minőségbiztosítás jelentősége az élet minden területén egyre nagyobb lesz. A műszaki élet területén dolgozó mérnökök számára is rendkívül fontos, hogy a minőséggel, a minőség-technológiával kapcsolatos fogalmakat ismerjék és azokat alkalmazni is tudják.

A minőség fogalmat a mindennapi életből mindannyian ismerjük, pontos meghatározása mégis igen nehéz feladat. E fogalom a minőségbiztosítás története során állandóan változott, fejlődött. Az értelmezés súlyponti kérdése az idők folyamán számos változáson ment át, kezdetben elsősorban a szabványoknak való megfelelés alapján definiálták a minőséget, majd a használhatóság, a költségek, a társadalmi és környezeti elvárásoknak való megfelelés lett a döntő kérdés. Ugyanilyen fejlődési folyamat figyelhető meg a minőség megvalósítását vizsgálva. Az ipari termelés kezdeteinél a termelés és az ellenőrzés még nem vált el szigorúan, maga a gyártásban szereplő ember végezte az ellenőrzést is. Későbbi fázisra a műszaki ellenőrzési részlegek (MEO) megjelenése a jellemző, a termelés és minőségellenőrzés ezzel már elvált egymástól, az ellenőrzést a gyártási folyamat végén végezték, s az ellenőrzésnek a fő célja a selejtet előállító személy megtalálása (és megbüntetése) volt. A következő lépcsőben megkezdődött a minőség szabályozása, melynek elsődleges célja nem a hibát elkövető személy megtalálása, hanem a gyártási folyamat előírt határok közé való visszavitele lett. E fázis jellemző módszerei a statisztikai minőség-ellenőrzés, majd a statisztikai folyamat-szabályozás **(SPC)** voltak. A múlt század utolsó harmadában jelent meg a teljes körű minőségszabályozás, illetve minőségirányítás.

11.1.2. Minőségellenőrzés

A minőségellenőrzés célja mindig az új termékek megfelelőségének a vizsgálata: a megfelelőséget a termék tulajdonságai alapján kell eldönteni. A minőségellenőrzés során azt kell megvizsgálni, hogy a termék jellemzői mennyire felelnek meg a vonatkozó szabványokban, szerződésekben, ellenőrzési utasításokban megfogalmazott követelményeknek.

A minőségbiztosítás témaköréhez szervesen hozzátartoznak az e területen alkalmazható modellezési és méréstani módszerek ismerete, ezek

eszközeinek használata. E területen különösen nagy jelentősége van a minőségre vonatkozó szabványok megfelelő ismeretének.

11.1.3. Teljes körű minőségirányítás (TQM)

A minőségbiztosítás alapvető fogalma a teljes körű minőségirányítás, a Total Quality Management (=TQM), a minőség elérésének általános vezetési módszere, ami a szervezet teljes működését átfogja. Segítségével egy cég egészének hatékonysága, rugalmassága, versenyképessége javítható. Fogalma először az 1980-as évek közepén jelent meg, elnevezésében és tartalmában az Amerikában 1961-ben megfogalmazott Total Quality Control módszerére épít. Ez is tulajdonképpen a hagyományos minőségpolitika különböző részfeladatait foglalja egységbe. Ezek a

- minőségtervezés,
- minőségirányítás,
- minőségbiztosítás,
- minőség javítás.

A **minőségtervezés** célja a megfelelő minőség eléréséhez szükséges tevékenységek előzetes rögzítése. Ehhez szükség van a tevékenységek megfelelő részletezésére, a követelmények alapján a megfelelő minőségi célkitűzések megfogalmazására, valamint megfelelő munkamódszerek kialakítására. E feltételeket a **minőségirányítás** teremti meg. A minőséggel kapcsolatos tevékenységeknek a vállalat felépítésébe, munkafolyamataiba való beépítése a **minőségbiztosítás** feladata. Ennek természetesen megvan a következménye a teljes vállalatot átfogó menedzsment rendszerben is. A minőségirányítás fő célja a **minőség** állandó **javítása.** Ide tartoznak mindazok az intézkedések, amelyek a vállalaton belüli folyamatok hatékonyságának, gazdaságosságának növelésére irányulnak. Ezzel megfelelően nagy haszon érhető el mind a vállalat, mind a vevők részéről.

Ez a minőségirányítási rendszer szabványban is meghatározza a minőségi követelményeket, amelyek állandóan változnak, fejlődnek. A TQM tekinthető a legáltalánosabb minőség-stratégiának. Az ügyfelektől a szervezet dolgozóin keresztül a beszállítókig a szervezet valamennyi területét magába foglalja és integrálja.

Vizsgáljuk meg az elnevezés három fő elemét részletesen:

- Átfogó jelleg (Total),
  - vevőorientáltság (megfelelő kommunikáció a vevőkkel, a vevők igényeinek kielégítése, mint a minőség mértéke),
  - munkatárs-orientáltság (a minőség nem egyetlen osztály, hanem a szervezet valamennyi munkatársának feladata)
  - társadalom- és környezet-orientáltság,
  - helytől és funkciótól való függetlenség.
- Minőség (Quality)
  - a szervezet minősége (a munkatársak megfelelő képzettsége, továbbképzése),
  - a folyamatok minősége (a megrendelők és szállítók közötti kapcsolatok hálózatának kiépítése)
  - a munka minősége (valamennyi folyamat állandó javítása),
  - a termékek minősége (megelőző intézkedések a hibák elkerülésére).
- Menedzsment (vezetés értelmében véve; Management)
  - a vezetés minősége (top-down szemlélet megvalósítása, a legfelsőbb vezetés bekapcsolásával),
  - minőségpolitika, minőségi célkitűzések (minőség javítása mint hosszú határidejű folyamat),
  - csoport-munkára való készség, tanulási készség (a munkafeltételek biztosítása, a csoportmunka, a részvétel támogatása).

A TQM fontos célkitűzése a vevők, illetve szolgáltatásokat igénybevevők elvárásainak minél tökéletesebb kielégítése. A TQM – mint rendszer – fontos jellemzője az élet különböző területein megfigyelhető változások figyelemmel kísérése, a legkülönbözőbb javító módszerek széleskörű alkalmazása. A teljes rendszer mögött üzleti szemlélet húzódik meg, ami a versenyképesség növelését tűzi ki célul. Fontos a minőségbiztosítási kérdések mögött húzódó gazdasági szempontok állandó szem előtt tartása.

A TQM a szervezet valamennyi tagjának közreműködésére támaszkodó menedzsment-módszer, amelynek középpontjában a minőség áll, célja pedig az üzletfelek elégedettsége alapján hosszú távú üzleti siker. A „valamennyi tag” kifejezés a szervezeti hierarchia valamennyi szintjének valamennyi helyén közreműködő személyt jelenti. A TQM módszer sikerének fontos előfeltétele, hogy a szervezet legfelsőbb vezetése valóban meggyőzően végezze munkáját és a szervezet valamennyi tagja megfelelően képzett és iskolázott legyen. Az átfogó minőség-menedzsment minőség fogalma valamennyi üzleti cél elérését jelenti.

A TQM minőségközpontú irányítási rendszer alkalmazása során világosan látni kell, hogy nemcsak műszaki, technológiai kérdések megoldására, hanem ezekkel párhuzamosan megfelelő rendszerszintű szervezési és személyzeti problémák kezelésére is szükség van. Alapvető cél a vevők, a szolgáltatások igénybevevői elégedettségének elérése, valamennyi folyamat és alkalmazott bevonásával. E célok elérése a termékek folyamatos javításával, a költségek minimalizálásával kell, hogy történjen.

A minőségbiztosítás ilyen módon egy új viselkedési, vezetési és gondolkodásmódot jelent, amelynek lényege a vevői igények kielégítése, a folyamatok állandó javítása a teljes személyi állomány teljes körű bevonásával.

11.2. A minőségbiztosítás elméleti kérdései

A következőkben a minőséggel kapcsolatban mindig termékről beszélünk, de pontosabb definíció szerint ilyenkor mindig az általánosabb „átadandó”-t kellene említeni, ami lehet egy valóban megfogható termék, feldolgozott anyag, hardver vagy szoftver, szolgáltatás, szellemi termék. A minőségbiztosítás felöleli a szolgáltató ipar, kereskedelem, a közigazgatás, oktatás, a jogi, pénzügyi és orvosi gyakorlat és egyéb szakértői szolgáltatások területét is.

Hasonlóan, az egyszerűség kedvéért mindig gyártót említünk és ez alatt értjük az átadandó előállítóját. A minőségbiztosításban fontos szerepet játszó szerződésben e két fél szerepel, s a szerződés e két fél között létrejött nem feltétlenül írásbeli megállapodás valamilyen értéket képviselő termék előállítására, illetve az érte járó ellenszolgáltatásra vonatkozóan.

A termék minőségéért a szerződéses kapcsolatban álló mindkét fél felelős. Az előállító, gyártó felelős az előállítás folyamatáért, minden részfolyamatáért, a folyamatok kívánt eredményeiért és mellékhatásaiért. Fontos, hogy az előállítási folyamat során hozott döntések, a döntéshozók és felelősök nyomon követhetők legyenek. A felhasználó elsősorban az ellenszolgáltatásért felelős, de a minőség szempontjából fontos feladata a megfelelő specifikáció összeállítása, annak karbantartása és a gyártóval való együttműködés a gyártás során.

A specifikáció fontossága különösen szembetűnő biztonságkritikus termékek előállítása során. A követelmények összeállítását leggyakrabban verbális módszerrel végzik, ami magában hordja a szóbeli megfogalmazások pontatlanságából származó hibák lehetőségét. Ha különösen nagy érdekek fűződnek a specifikáció hibamentességéhez, akkor lehetőség szerint a pontosabb fél- (= szemi-) formális, illetve formális módszereket kell alkalmazni.

A biztonságkritikus rendszerek minőségbiztosítása során a kétszereplős szerződésmodell kibővül a hatóság közreműködésével. A megfelelő minőség elérésére a hatóság jóváhagyása, engedélye is szükséges a rendszer használatbavételéhez.

A minőségbiztosítás fontos előfeltétele, hogy a valóságban előforduló bonyolult rendszereket rendszer-szemléletben tudjuk vizsgálni és minél egyszerűbb modellekkel tudjuk közelíteni. A rendszerszemléletű vizsgálat szempontjából legfontosabb modellek az ún. fekete doboz és a szerkezeti modell. Az előbbi csupán a bemenetekre adott kimeneti válaszokat vizsgálja, utóbbi a rendszerelemek struktúráját, az elemek közötti kapcsolatokat vizsgálja. A vizsgálandó rendszer struktúrájának ismeretében a minősítés során a termék választott tulajdonságait kell lehetőleg számszerűen leírni. Így a minőségbiztosítás szempontjából fontos kérdés a termék tulajdonságainak mérhetősége.

A minőségi vizsgálatok elvégzése, a termékek tesztelése során előírt körülmények között kell meghatározni azok jellemzőit. A tesztelés fontos műveletei a különböző mérések. A tesztelés volumene az ún. tesztfedéssel jellemezhető. A tesztelés mértékének meghatározásához meg kell határozni a rendszer teljes körű vizsgálatához szükséges lépések összes számát, ez adja a ún. teljes teszt teret. A ténylegesen végrehajtott vizsgálati lépésekkel csak a teljes teszttér egy részét lehet lefedni, a tesztfedés mértéke a ténylegesen végrehajtott és összes tesztlépések számának a viszonyszáma.

A tesztelés fontos eszköze a mérés. A tesztelés során összehasonlítjuk a termék adott és megkívánt jellemzőit. A tesztelés csak akkor lehet sikeres, ha ezek a tulajdonságok mérhető formában meghatározottak. Amennyiben bizonyos tulajdonságok egy része nem áll rendelkezésre mérhető formában, akkor megfelelő pontrendszer kialakításával lehet a számszerűsítést elvégezni (tenderek összetett jellemzői esetén gyakran van ilyenre szükség). Ezek a mutatószámok viszont óhatatlanul tartalmaznak szubjektív elemeket, emiatt az ilyen eredmények gyakran képezik vita tárgyát. A tesztelés akkor megfelelő, ha viszonylag kevés vizsgálati lépéssel a hibák zöme felismerhető (célszerű, optimális tesztek kialakítása fontos, érdekes mérnöki feladat). A tesztelésnek számos formája van:

- ellenőrzés,
- vizsgálat,
- igazolás (verifikáció),
- érvényesítés, jóváhagyás (validáció),

- minősítés (kvalifikáció),
- tanúsítás (audit).

A fenti módszerek közül a biztonságkritikus rendszerek esetén az ún. biztonságigazolás és alkalmasság igazolás jelentőségét kell kiemelni. A kettő közötti határvonal megállapításához a specifikáció két fajtájának megkülönböztetése szükséges. A felhasználó igényeit az ún. követelmény specifikációban foglalja össze, ez alapján a gyártó cég készíti el a gyár(tás)i specifikációt. A biztonságigazolás során a gyári, az alkalmasság igazolás során pedig a felhasználói specifikáció feltételeinek teljesülését kell ellenőrizni. Belátható módon eredményes biztonságigazolás után eredménytelen alkalmasság-igazolás úgy fordulhat elő, ha a két specifikáció nem fedi teljesen egymást. Ezért van különös jelentősége a már említett formális specifikációs módszereknek.

A TQM tulajdonképpen a teljes vállalat bevonását jelenti a fent megfogalmazott feladatok megoldásába. A minőségirányítási rendszer feladatainak dokumentációját a **minőségirányítási kézikönyv** jelenti. E kézikönyv tartalmazza többek között a vállalat minőségpolitikájának alapvető elveit és a vállalat dolgozóinak felelősségére és illetékességére vonatkozó szabályozásokat. Ehhez jönnek még a folyamatok hatékony tervezésének, végrehajtásának és irányításának szervezeti kialakítására vonatkozó megállapítások. Ez a kézikönyv vonatkozhat a teljes vállalatra, vagy csupán egyes részterületeire is. Nem szükséges a kézikönyv tartalmának a vállalat összes folyamatát lefednie, elegendő csupán a folyamatok kapcsolatait, kölcsönhatásait leírni. Tartalmazhat melléklete(ke)t is, amelyben az alkalmazandó formanyomtatványokat adhatják meg. A minőségirányítási kézikönyv felépítésében és tartalmában értelemszerűen alkalmazkodik az ISO 9001:2000 szabványban leírtakhoz. Kiadását a vállalat vezetősége kezdeményezi, mindig két kiadás készül. Az egyik a vállalati menedzsment és a dolgozók számára, tehát belső használatra, amit állandóan aktualizálni kell, főleg az érvényes eljárások, a munkafolyamatok és a vizsgálati módszerek tekintetében. Ennek a kiadásnak mindig rendelkezésre kell állnia a dolgozók számára. A kiadás formáját nem írja elő pontosan a szabvány, megjelenhet papír, illetve elektronikus formában egyaránt. A másik, külső célokra szánt kiadás bemutatja a céget a megrendelők számára, ugyanakkor vásárlói tájékoztatónak és reklám anyagnak is tekinthető. Természetesen gondoskodni kell arról is, hogy a vállalt belső információi, titkos anyagai

ne kerüljenek nyilvánosságra. Ezen túl a minőségirányítási kézikönyv a szállítók és megrendelők közötti szerződések alapjául is szolgálhat.

A megfelelő minőség elérésére az előállító szervezetnek létre kell hoznia s megfelelően dokumentálva fenn kell tartania egy minőségirányítási rendszert. E rendszer kialakításának módját a minőségbiztosítási szabványok tartalmazzák.

11.3. A minőségbiztosítás szabványosítási kérdései

11.3.1. A minőségbiztosítási szabványrendszerről általában

A minőségirányítási rendszerrel szemben támasztott követelmények csak jól dokumentált rendszerrel teljesíthetők. A jól dokumentált minőségi rendszer biztosítja egyrészt a vevők, másrészt a szervezet igényeinek teljesíthetőségét. A vevők számára megteremti azt a bizalmat, hogy a szervezet képes a kívánt terméket a megfelelő minőségben előállítani. A szervezet felé pedig lehetővé teszi, hogy a megfelelő minőséget elfogadható költséggel, a rendelkezésre álló erőforrások hatékony felhasználásával érje el. A folyamat jól dokumentáltsága pedig biztosítja és igazolja, hogy a termék előállításának teljes folyamata szabályozott körülmények között zajlott le, így a minőség, a költség és a határidő jól kézben tartható.

A minőséggel kapcsolatos fogalmak egységes értelmezhetősége érdekében e fogalmakat szabvány rögzíti. A nemzetközi gyakorlatban legelterjedtebben alkalmazott minőségi szabvány az ISO 9000-es sorozat, melynek segítségével lehetővé válik, hogy a vállalatok meghatározzák és kifelé deklarálják a megfelelő minőséget. Az ISO 9000-es szabványrendszer segítségével válik lehetővé az adott területen szabványokban rögzített követelmények kielégítése, a termékek, szolgáltatások megfelelősége, a hibák továbbterjedésének megakadályozása és a gyártással, termeléssel, szolgáltatás előállítással kapcsolatos mindenkori helyzet dokumentálása és ellenőrzése.

Az ISO szabványrendszer alkalmazásával elérhető eredmény a különböző területeken elég különböző. Alkalmazása már több évtizedes múltra tekint vissza. A genfi ISO (=International Standardisation Organzation) szabványosítási szervezet 1987-ben bocsátotta ki a 9000-es sorozatot, ami aztán hamarosan bevonult a német (DIN), az európai (EN) és egyre inkább a nemzeti szabványok körébe is (hazai vonatkozásban például az MSZ-EN sorozat, s az eredeti kiadásnak megfelelő MSZ EN 29000:1991 szabvány).

Az ISO szabvány-sorozat kialakítása során az angol szabványokat vették leginkább figyelembe – alapul a hadiipar számára kidolgozott BS 5750 szabvány szolgált és a felhasználók körében is Nagy-Britannia jár élen. A kiadott tanúsítványok száma 1994-es adatok szerint háromszor annyi, mint egész Európában és a világon kiadott bizonyítványoknak több mint 2/3 része származik Nagy-Britanniából.

A szabványrendszer hosszabb fejlődési folyamat lezárásaként jelenhetett meg és elterjedése igen gyors volt. A megjelenés évében már 8 ország átvette a teljes szabvány-sorozatot, két további ország (Kanada és India) pedig csupán a 9004-es részét. A következő évben újabb 8 országgal bővült a szabványt alkalmazó országok köre.

Az ISO 9000 szabványrendszer elsősorban nem a termékek minőségének vizsgálatát, hanem a termelési folyamatok és a menedzsment teljesítmények átláthatóvá tételét célozza meg. Ezeket a szabványokat termelő és szolgáltató üzemekre egyaránt alkalmazni lehet. A szabvány lényege az eljárás meghatározása és vizsgálata, valamint a hibák felismerése és elkerülése rendszerének fejlesztése. E rendszer írásos formában történő dokumentálására a szabvány a korábban már említett minőségirányítási kézikönyvet írja elő. Az ISO 9000 szabványrendszer által előírt nyomtatványok, illetékességek, a megfelelő minősítéssel rendelkező munkahelyek leírása ebben megtalálható.

Az ISO 9000 szabványrendszer szerint összeállított dokumentáció a gyártó (szolgáltató) és a megrendelő közötti közös nyelv megteremtésében jelent nagy segítséget. Ezzel lehetőség nyílik arra, hogy a minőségbiztosítás egyes elemeit illetően megállapodások születhessenek és azokat objektív módon vizsgálni lehessen. A fő cél, hogy az üzemen belüli teljes életciklusra kiterjedő folyamatot átláthatóvá lehessen tenni (a megbízástól, szerződés létrejöttétől, a tervezés, fejlesztésen, termelésen és vizsgálatokon át a raktározásig, csomagolásig, szállításig, kereskedelemig, vevőszolgálatig). A rendszeres ellenőrzések (ún. auditok) során kell meghatározni, hogy a minőségi kézikönyv előírásait valóban teljesítették-e.

Az ISO 9000 szabványrendszer gyors elterjedését nem utolsósorban a szavatossági jog újabb előírása segítette elő, miszerint valamely termék által okozott károkért a gyártót csak akkor nem terheli felelősség, ha a termék gyártásának időpontjában nem volt látható a bekövetkezett kockázat, vagy ha a gyártó igazolni tudja, hogy a biztonsági probléma nem az ő üzemében keletkezett. Tehát kár bekövetkezésekor a gyártói felelősségi igényeket csak akkor lehet elkerülni, ha a gyártó cégnél minden biztonság-

kritikus tevékenység megfelelően, precízen és áttekinthető formában dokumentálva van.

11.3.2. A minőségbiztosítás különböző koncepciói

A modern minőségirányítási szabványokat eredetileg a hadiipar számára dolgozták ki, majd angolszász területen jelentek meg az első, a civil szféra számára érvényes minőségügyi szabványok. 1979-ben jelent meg a BS 5750, ami az ISO 9000-es szabvány-sorozat közvetlen előzményének tekinthető. Első változata a CEN európai szabványtestület által kiadott EN 29000:1987 jelzésű szabvány volt, majd átdolgozott formában 1994-ben adták ki EN ISO 9000 jelzéssel.

A minőségbiztosítási koncepciót továbbra is elsősorban az ISO 9000 szabványrendszer alapján kívánjuk tárgyalni. Itt célszerű azonban megemlíteni, hogy ez nem az egyedül alkalmazott minőségügyi szabványrendszer. Ennek alapján más minőségügyi rendszereket is kidolgoztak, amelyek egy-egy speciális területen kerülnek alkalmazásra. Ilyen szabványrendszer például az ún. QS 9000 szabvány, ami az autóipari cégek vonatkozásában foglalja össze a minőséggel kapcsolatos elvárásokat. A QS 9000 szabvány egyrészt az autógyártással kapcsolatban már évek óta alkalmazott minőségügyi rendszerek, részint az 1987-ben megjelent ISO 9001-es szabvány felhasználásával készült. Első kiadása 1994-ben jelent meg. Érdekességként említjük, hogy ez a rendszer is az eredeti ISO 9001 szabvány 20 pontos követelményrendszerét tekintette kiinduló pontjának.

11.3.3. Az ISO 9000 szabványrendszer fejlődése

11.3.3.1. A szabványrendszer kialakulása

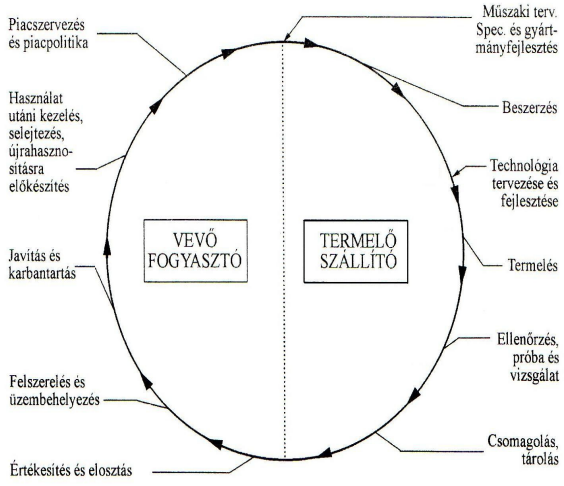
Bár érvényessége már megszűnt, de célszerű röviden az eredeti változatot is megismerni. A szabvány család szabványainak egy része közvetlenül a termék harmadik fél által történő tanúsításának céljára szolgál, más részük pedig irányelveket adnak a minőségi rendszer kialakítására vonatkozóan.

Az ISO 9000 szabványrendszer eredetileg 5 részből állt (az ISO 9000-től az ISO 9004-ig). Az első, az ISO 9000 szabvány általában leírta, hogy milyen módon kell a többi szabványt alkalmazni. Az ISO 9001 – ISO 9003 szabványok három különböző minőségbiztosítási koncepciót tartalmaztak. Az ISO 9001 szabvány a tervezés, fejlesztés, szerelés és közönségszolgálat területére írta elő a minőségbiztosítás módját. Az ISO 9002 a termelés és szerelés, az ISO 9003 pedig csupán a végső vizsgálatra tartalmazott minő-

ségbiztosítási rendszert. Ezek a szabvány-fejezetek szolgáltak a tanúsítások alapjául.

Az ISO 9004 szabvány ajánlásokat adott egy minőségbiztosítási rendszer felépítésére és leírta az üzemek által teljesítendő követelményeket az ISO 9001, 9002 és 9003 szabványok teljesítéséhez. A 9004 szabvány második része a minőségbiztosítási rendszer szolgáltatások területére történő átvihetőségére adott ajánlásokat. Az ISO 9001 szabvány leírta a tervezés, fejlesztés, gyártás, szerelés és vevőszolgálat területén alkalmazandó minőségmenedzsment modelljét. Ez a szabvány 20 pontban, 20 ún. minőségmenedzsment-elem megadásával foglalta össze a szállító cégek legátfogóbb minőségbiztosítási követelmény-rendszerét.

Az ISO 9001 – 9003 szabványok nem termékre vonatkoztak, hanem teljes vállalatirányítási rendszerre és a vállalat tevékenységi körének megfelelően került sor alkalmazásukra. Mivel a megfogalmazások túl általánosak voltak, kiadták a magyarázatokat tartalmazó 9000 (majd később a 9000-1 és 9000-2) szabványt, amely ismertette a három említett szabvány alkalmazásának módját. Hasonló szerepe volt az ISO 9004 jelű szabványnak is, ami szintén a minőségirányítási rendszer céljára, bevezetésének módjára adott eligazítást. Ez utóbbi már a teljes életciklusra vonatkozóan írja elő a minőségbiztosítás feladatait, megfogalmazza a minőségirányítás életciklus modelljét, az ún. minőséghurkot (11-1. ábra)



11-1. ábra: A minőségi hurok

Az ISO 9000 szabványrendszer kialakulása és a kezdeti években megfigyelhető gyors elterjedése mutatta annak életképességét. Az ISO Nemzetközi Szabványügyi Szervezet tevékenységének fontos része az általuk kidolgozott szabványok rendszeres (általában 5 évenkénti) felülvizsgálata. Így biztosítják szabványaik mindenkori korszerűségét.

Az ISO TC 176-os bizottság „Vision-2000" nevű stratégiai programja alapján az ISO 9000 szabványrendszer felülvizsgálatát az alábbi szempontok alapján végezte el:

- a szabvány szövegének pontosítása, tökéletesítése,
- az alkalmazás során felmerült hibák, hiányosságok megszüntetése,
- újabb elemek bevonása a szabványrendszerbe.

Az első nagy felülvizsgálat 1994-ben történt, melynek során az eredetihez képest a lényegi rész változatlansága mellett a követelmények pontosabbak, rendezettebbek lettek. A három modellszabvány egységes szerkezetű lett, az előírást tartalmazó fejezetek száma nőtt.

A módosulások során a 9000-es ún. vezérszabvány (Minőségirányítási és minőségbiztosítási szabványok cím alatt) több részszabványra bomlott, az alábbiak szerint:

- ISO 9000-1:1994 (magyar megfelelő: MSZ EN ISO 9000-1)
  1. rész: Irányelvek a kiválasztáshoz és az alkalmazáshoz,
- ISO 9000-2:1993 (magyar megfelelő: MSZ ISO 9000-2)
  2. rész: Általános irányelvek az ISO 9001, ISO 9002 és ISO 9003 szabványok alkalmazásához,
- ISO 9000-3:1991 (magyar megfelelő: MSZ ISO 9000-3)
  3. rész: Irányelvek az ISO 9001 alkalmazásához a szoftverfejlesztés, ~szállítás és ~karbantartás területén,
- ISO 9000-4:1993 (magyar megfelelő: MSZ ISO 9000-4)
  4. rész: Útmutató a megbízhatósági program irányításához.

Az ISO 9001, 9002 és 9003 szabványok Minőségügyi rendszerek címmel az ISO modelleket a következők szerint foglalja össze:

- ISO 9001:1994 (magyar megfelelő MSZ EN ISO 9001)
  A tervezés, a fejlesztés, a gyártás, a szerelés és a szolgáltatás minőségbiztosítási rendszerének modellje,

- ISO 9002:1994 (magyar megfelelő MSZ EN ISO 9002)
  A gyártás, a szerelés és a szolgáltatás minőségbiztosítási rendszerének modellje,
- ISO 9003:1994 (magyar megfelelő MSZ EN ISO 9003)
  A végellenőrzés és a vizsgálat minőségbiztosítási rendszerének modellje.

A minőségirányítási és minőségügyi rendszerelemeket az ISO 9004 szabvány foglalja össze a következők szerint:

- ISO 9004-1:1994 (magyar megfelelő MSZ EN ISO 9004-1) 1. rész: Irányelvek,
- ISO 9004-2:1994 (magyar megfelelő MSZ EN ISO 9004-2) 2. rész: A szolgáltatás irányelvei,
- ISO 9004-3:1994 (magyar megfelelő MSZ EN ISO 9004-3) 3. rész: Irányelvek a feldolgozott termékekhez,
- ISO 9004-4:1994 (magyar megfelelő MSZ EN ISO 9004-4) 4. rész: Irányelvek a minőségfejlesztéshez.

Külön szabványok foglalkoznak a minőségügyi rendszerek felülvizsgálatával, mások pedig megadják a témakör terminológiáját, irányelveket adnak a minőségügyi kézikönyvek kidolgozásához, a mérőberendezések metrológiai jóváhagyására (akkreditált laboratóriumok), az alkalmazható statisztikai módszerek kiválasztására.

Az 1994-ben végrehajtott szabvány-felülvizsgálat alapján végzett módosítások eredményeképpen a szabványok új változata egyértelműbb, pontosabban megfogalmazott lett. További előnye volt a felülvizsgálatnak, hogy korábban nem szabályozott területek is bekerültek a szabványba. A változás tartalmi részét illetően előrelépést jelentett, hogy a szabványok felépítését közelítették egymáshoz: a 9002 és 9003 szabványok felépítése, tartalma a sorozat legrészletesebb tagjához, a 9001 szabványhoz közeledett. Ekkor jelent meg a 9002 szabványban a szolgáltatásokkal (vevőszolgálattal) kapcsolatos fejezet. A változások eredményeképpen a követelményszint általában emelkedett valamennyi rendszermodellben, a szabványok szerkezete logikusabb, tagoltabb lett, az új változatok általánosságok helyett konkrétabb megfogalmazásokat tartalmaznak, megszűntek bizonyos felesleges szabályozások. Bővült a szabványok közötti kereszthivatkozások száma is.

11.3.3.2. A szabványrendszer továbbfejlesztését (ISO 9000: 2000) sürgető szempontok

Az új szabvány kidolgozását a következő indokok tették szükségessé:

- A régi szabványsorozat egyes tagjainak alkalmazási területe különböző volt, az új szabványsorozatban az ISO 9001: 2000 helyettesíti az ISO 9001, ISO 9002 és ISO 9003 szabványokat. Ezen új szabvány alkalmazási területét a vállalat jellegétől függően határozták meg.
- A korábbi szabványsorozat gyártásközpontúságával szemben szükséges volt a szolgáltató szervezetekre, intézményekre érvényes követelményeket is bevonni a szabványba.
- A korábbi szabvány központjában a minőség szempontjából rendkívül fontos minőségügyi rendszer állt, az új szabvány a vevők elégedettségét teszi elsődleges szemponttá. E szemlélet változás miatt a minőségbiztosítási rendszer helyett a szabvány a minőségirányítás követelményeit foglalja össze. Az új rendszer középpontjában a vevői igények vannak, a vállalt felső vezetésének a feladata, hogy a vevői igényeket követelményekké alakítsa.
- A régi szabvánnyal szemben a korszerű minőségügyi filozófia, a TQM-modell elveinek érvényesítése a cél.

11.3.3.3. Az új és régi szabványok kapcsolata

Célszerű röviden táblázatosan összefoglalni a régi és az új szabványok kapcsolatát:

ISO 8402 ISO 9000-1 ISO 9000-2	⇒	ISO 9000:2000
ISO 9001 ISO 9002 ISO 9003	⇒	ISO 9001:2000
ISO 9000-2 ISO 9000-3 ISO 9004-1 ISO 9004-2 ISO 9004-3 ISO 9004-4	⇒	ISO 9004:2000
ISO 9004-4 eszközök	⇒	Megszűnt

9000-3	⇒	Értelmező szabvány
ISO 10012-1	⇒	Megmaradt
ISO 10013	⇒	Műszaki jelentés
ISO 10011-1 ISO 10011-2 ISO 10011-3 ISO 14010 ISO 14011 ISO 14012	⇒	ISO 19011:2001

11.3.3.4. Az új szabvány alapelvei

A korábban külön szabványban szereplő minőségirányítási és minőségbiztosítási szótárt (ISO 8402) az ISO 9000:2000 szabvány első része tartalmazza. A használatos fogalmakat a következő témaköri bontásban foglalja össze:

- minőség,
- irányítás,
- szervezet,
- termék és folyamat,
- jellemzők,
- megfelelőség,
- dokumentumok,
- vizsgálat,
- audit.

Az új szabvány a folyamat eredményeként létrejövő termékeknek négy kategóriáját különbözteti meg:

- hardver,
- szoftver,
- szolgáltatás és
- feldolgozott anyag.

Adott termék a fenti kategóriák közül nemcsak egybe tartozhat, ilyenkor azt a meghatározó kategóriába kell besorolni.

Az új szabványsorozat 8 alapelvet fogalmaz meg, ezek a:

1. folyamatszemléletű megközelítés,
2. rendszerszemlélet az irányításban,
3. tényeken alapuló döntéshozatal,
4. vezetés szerepe a feltételek biztosításában,
5. vevőközpontúság,
6. folyamatos fejlesztés
7. a munkatársak bevonása a folyamatba, a döntéshozatalba,
8. kölcsönösen előnyös kapcsolatok a beszállítókkal.

Az ISO 9000 a szabvány szerves részeként összefoglalja a minőségirányítás TQM szemléletű alapelveit. A teljes szabványrendszerre a rendszer- és folyamat-központú szemlélet a jellemző.

Ennek megfelelően a rendszert egymáshoz kapcsolódó folyamatok összességének (hálózatának) tekinti, melyek az erőforrásokkal a megfelelő eljárások felhasználásával a bemeneteket úgy alakítják át kimenetekké, hogy közben hozzáadott értéket állítanak elő. A szabvány meghatározza a minőségirányítási rendszer értékelésének fő módszereit:

- auditálás,
- vezetőségi vizsgálat és
- önértékelés.

A minőségirányítási rendszer összetett folyamatnak tekinthető, melynek bemenetét a „vevők" igényei, követelményei jelentik. Gyakran csak az igények fogalmazódnak meg explicit formában, ezek alapján a szervezetnek kell kialakítania a követelményrendszert, végül ebből kell meghatároznia a termék jellemzőit. Az ábra szerint a vevői igényeknek követelményekké alakítása a vezetőség feladata. A szükséges erőforrások felhasználásával, megfelelő irányításával létrehozható a termék (szolgáltatás), amit a vevőkhöz kell eljuttatni. Ez jelenti a folyamat kimenetét. Fontos, hogy a termékkel a vevő elégedett legyen. A minőségirányítás folyamatrendszere a kimenet megjelenése után folytatódik a vevők visszajelzéseinek felhasználásával, az ehhez szükséges mérés, elemzés és javítás folyamatával. Ez a folyamat a termékre (szolgáltatásra), az ezt előállító folyamatokra és a vevői visszajelzésekre vonatkozó adatok elemzésével, értékelésével a minőségirányítási rendszer javítását eredményezi. A minőségirányítási rendszer fenti értelmezésével az ISO 9001:2000 szabvány négy fő folyamateleme a vezetőség felelősségére, az erőforrások irányítására, a termék (szolgáltatás)

megvalósítására, a rendszer továbbfejlesztésére (mérésre, elemzésre és javításra) vonatkozó követelményeket foglalja össze. E folyamatelemek megfelelnek az ún. PCDA-ciklusnak. Az erőforrásokkal való gazdálkodás, ami a vezetőség feladatát jelenti, képezi a tervezési fázist (Plan = **P**), ezután következik a termék előállításához szükséges folyamatok végrehajtása, irányítása (Do = **D**). A folyamatok lebonyolódását mérni, a mérési eredményeket elemezni kell (Check = **C**), és ennek eredménye alapján elvégezhető a javító, fejlesztő tevékenység, és megtörténhet a folyamatba való beavatkozás (Act =**A**). A felülvizsgálat és a vizsgálat eredményeinek hasznosítása jelenti a minőségirányítási rendszer fejlesztését.

Az ISO 9000 szabványcsalád 2000 évi új kiadásának fontos jellemzője a teljes folyamatirányítási rendszer kiépítése a vevői igények felmérésétől kezdve a vevői megelégedettség figyelemmel kíséréséig és a folyamatos fejlesztés megvalósításának követelménye. Az új szabvány sajátosságai tehát az alábbiak szerint foglalhatók össze:

- Az ISO 9001:2000 jellegzetességei:
  - folyamat-központú szemlélet és megközelítés,
  - erőforrások, emberi erőforrások külön kezelése,
  - a rendszer folyamatos fejlesztésére, tökéletesítésére vonatkozó követelményt megfogalmazása,
  - a felső vezetés szerepének nagyobb hangsúlya.
  - a Shewhart[1]-Deming[2] féle ún. PDCA ciklus szerinti felépítés,

  Ugyanakkor
  - nem célja, hogy a minőségirányítási rendszer szerkezetét, vagy dokumentációs rendszerét egységesítse,
  - a rendszer dokumentációjának mértékét a szervezet nagyságától, típusától, a folyamatok bonyolultságától, kölcsönhatásaitól, valamint a személyzet kompetenciájától függően kell meghatározni.
- Az ISO 9004:2000 jellegzetességei:
  - Követi a 9001 szabvány felépítését,
  - Középpontjában a folyamatos fejlesztés szükségessége van, míg az eddigi szabvány csak a rendszer bevezetésére vonatkozó ajánlásokat tartalmazta.

[1] Shewhart, Walter.A.: Az USA Bell laboratóriumának mérnöke volt az 1920-as években, ő tekinthető a statisztikai folyamatszabályozás kidologozójának.
[2] Deming, W. Edwards: a minőségbiztosítás nagy alakja, Shewhart tanítványa, az ő nevéhez kötik a PDCA ciklus megfogalmazását, ami azonban már Shewhart-nál is szerepelt.

- A hatásosság és a hatékonyság kettős követelményét említi, szemben a 9001-es szabvánnyal, amely csak a hatásosságot (az elérendő eredményt) követeli meg.
- A vevőközpontúság kizárólagos említése helyett az összes érdekelt fél (munkatársak, tulajdonosok, beszállítók és a társadalom) igényeinek kielégítését tűzi ki célul.
- Fenti igények kielégítésére a termék megfelelősége mellett annak használhatóságát, megbízhatóságát, a szállítás feltételeit, a vevőszolgálati ellátottságot és a teljes életciklus-költséget is javasolja figyelembe venni.
- Útmutatást és mintakérdéseket ad az önértékelés végzéséhez („A" melléklet)
- Bemutatja a folyamatos fejlesztés két alapvető módszerét (Stratégiai áttörési projektek alkalmazása és a kis lépésekben megvalósítható folyamatos fejlesztés a „B" melléklet szerint).

Az ISO 9001 és 9004 a minőségirányítási rendszerekre együttesen alkalmazandó szabvány-pár. Együttes bevezetése esetén a szervezet haszna valószínűleg nagyobb lenne, mintha csak az egyiket alkalmaznák. Mindkét szabvány használható külön-külön is. A két szabvány tárgyköre különböző, de az együttes használat megkönnyítésére általános felépítésük hasonló.

Az ISO 9001 célja, hogy meghatározza a minőségirányítási rendszernek azokat a minimális követelményeit, amelyek teljesítése a vevő megelégedettségéhez szükséges. A szervezet e szabvány segítségével tehát azt a képességét is bizonyíthatja, hogy képes a vevői követelmények kielégítésére.

Az ISO 9004 célja az, hogy útmutatást adjon a vezetőségnek a minőségirányítási rendszer alkalmazásához és ezzel javítsa a szervezet általános eredményességét. Az útmutatás kevésbé vonatkozik a minőségirányítási rendszer kialakítására és működtetésére, a hangsúly a folyamatos fejlesztésen van. Az ilyen rendszer várhatóan hatásosan és hatékonyan fog hozzájárulni a szervezet vevőinek elégedettségéhez és hasznára lesz más érdekelt feleknek is.

Az ISO 9004 útmutatásainak betartása az olyan szervezetek számára javasolt, amelyek vezetősége túl kíván lépni az ISO 9001 minimális követelményein és eredményességét tovább kívánja növelni.

11.4. A teljes körű minőségirányítás (TQM) megvalósításának módszerei, eszközei

11.4.1. Folyamatos javítás, fejlesztés

A TQM megvalósításának fontos eszköze a folyamatos fejlesztés, amelynek alapját a korábban már említett PDCA elv alkalmazása jelenti. A termék előállításának folyamatában minden ciklus végére a javítások eredményeképpen egy jobb minőséget érhetünk el. A folyamatos javítás elvének alkalmazása is Deming nevéhez fűződik. Deming mendzsment programja egy eredetileg az 1950-es években Japánban bevezetett vállalati filozófia, amelyet aztán Európában is egyre szélesebb körben alkalmaznak. E filozófia alapelemei talán nem is tekinthetők teljesen újaknak, de összességében mégis egy új minőségfilozófia megjelenését eredményezték. Ennek lényeges kiinduló pontja, hogy minden aktivitás folyamatként fogható fel, amit megfelelő módon javítani lehet. Nem elég csupán a menetközben felmerülő problémákat megoldani, hanem a teljes folyamat alapvető megváltoztatására van szükség a megfelelő minőség elérésére. Az ilyen radikális változtatásokat csak a vállalat vezetőségéből kiindulva lehet végrehajtani.

11.4.2. A hibamentesség programja (az ún. 0-hiba program)

Célja a lehető selejt-mentes, utólagos munkát nem igénylő termékelőállítás. A program kidolgozása Philip B. Crosby nevéhez fűződik (1961). A minőség gazdasági oldalának vizsgálata során ő azt a felfogást képviseli, hogy nem a minőség előállítása okozza a költséget, hanem a hibák és a követelmények nem teljesítése növeli a minőséggel kapcsolatos költségeket. A hibamentesség módszere arra alapoz, hogy az emberek sokkal inkább megközelíthetik a tökéletes munkavégzést, ha feladatuknak tekintik, hogy a kicsinységekre is ügyeljenek és a tévedéseket lehetőleg elkerüljék. „Tévedni emberi dolog” – szól a mondás, ezért mindennemű hiba elkerülése problematikus. De fontos a minőségbiztosítás nagy gondolkodóinak (Deming, Crosby stb.) az a véleménye, hogy a rossz teljesítmény okát általában nem az emberi tényezőkben, hanem a rendszerben kell keresni. Nem az embereknek, hanem a rendszernek kell megváltoznia ahhoz, hogy a hibák minél inkább elkerülhetők legyenek. Jóllehet valóban elkerülhetetlenek az emberi hibák, de nem kell normálisnak és elkerülhetetlennek tekinteni a hibák előfordulását. A munkakörülményeket kell úgy alakítani, hogy a munka ne igényelje a dolgozók állandó figyelmét. Ezt a folyamat megfelelően robusztus kialakításával lehet elérni. Ennek előfelté-

tele, hogy megfelelő stratégia álljon rendelkezésre a hibák elkerülésére. A hibák megakadályozására a leghatékonyabb intézkedések a fejlesztési és a konstrukciós fázisban hozhatók. Ennek megfelelően a TQM a vezetőség arra vonatkozó gondolkodásmódját jelentheti, hogy a hibákat lehetőleg el lehessen kerülni.

12. Esettanulmány az FMEA alkalmazásához

12.1. Bevezetés

Az ipar teljes területén tapasztalható a termékek és a gyártófolyamatok folyamatos fejlődése, ezért ahol csak lehetséges az FMEA módszer használata a lehetséges hibák felismerésére és megelőzésére még fontosabb, mint valaha. A korábbi termék-visszahívási kampányok tanulmányozása bebizonyította, hogy a helyesen alkalmazott FMEA projektek a termék-visszahívások nagy részét megelőzhetővé tette volna.

Az FMEA sikeres alkalmazásának egyik lényeges része a megfelelő időben történő elemzés. Ez azt jelenti, hogy az FMEA elkészítése egy „esemény előtti" tevékenység legyen és ne egy „esemény utáni" gyakorlás. Az FMEA igazi értékének eléréséhez az szükséges, hogy az elemzést azelőtt hajtsuk végre, mielőtt valamelyik lehetséges meghibásodás ténylegesen megjelenik a terméken vagy folyamatban. Így a felismert szükséges változások minimális költséggel és könnyen bevezethetőek, megelőzve ezzel a változásokkal általában együtt járó krízis helyzeteket. Az FMEA lehetővé teszi olyan intézkedések bevezetését, amelynek elmulasztása jelentős problémához vezetne. Célszerű az egyes FMEA-t végző csoportok közötti kommunikáció és koordináció.

Az FMEA elkészítése nem egyszerűen bizonyos formanyomtatványok kitöltését jelenti, sokkal inkább fontos a folyamat megértése, annak érdekében, hogy megelőzzük a lehetséges meghibásodások előfordulását és megtervezhessük azokat a tennivalókat, amelyek a folyamatok kézbentartását és ezzel együtt a vevők elégedettségét eredményezik. (Az FMEA készítésével kapcsolatos ábrák a jegyzet mellékletében, a 13. fejezetben találhatók. A melléklet 1. ábrája felvázolja az FMEA készítés elemeinek sorrendjét. Az ábrában szereplő táblázat fejléce hasonló, mint a következő két ábrán, az egyes meghatározásokhoz tartozó megjegyzéseket a következő két ábrával kapcsolatban ismertetjük a 12.3.4. illetve 12.4.4. fejezetekben.)

Alapvetően három olyan eset van, amikor az FMEA készítése ajánlott és mindegyiknek megvan a maga külön jelentősége.

1. Új termék, technológia vagy gyártófolyamat. Az FMEA ebben az esetben a teljes termékre, technológiára és gyártófolyamatra kell, hogy kiterjedjen.
2. Meglévő termék vagy gyártófolyamat módosítása (feltehetően ennek létezik már korábban elkészített FMEA elemzése). Ebben az esetben a módosításokra kell a figyelmet összpontosítani, a módosítás esetleges hatásaira a termék, a folyamat és az értékesítés utáni helyzet figyelembevételével.
3. Meglévő termék vagy folyamat új gyártási környezetben, helyszínen, vagy egy új alkalmazás (feltételezve, hogy létezik korábbi FMEA). Ebben az esetben a megváltozott környezetre, helyszínre vagy alkalmazásra kell összpontosítani a figyelmet.

Általában az FMEA elkészítésével kapcsolatos felelősség egy személyre szól, az FMEA elkészítése ennek ellenére egy csoport munkája kell, hogy legyen. A csoport lehetőséget teremt a megfelelő szaktudású emberek összehívására (például műszakiak, termelési szakemberek, a vizsgálatok specialistái stb.). Az FMEA tevékenységet az alaptevékenységért felelős mérnök kezdeményezi (termék-tervezés, technológia), ami lehet a szervezet, a szállító vagy más alvállalkozó felelőssége.

12.2. Az FMEA meghatározása

Az FMEA úgy definiálható, mint szisztematikus tevékenységek egy csoportja, amelyek fő célja:

- felismerni egy termék/folyamat lehetséges meghibásodásait és azok hatásait,
- javító intézkedések meghatározása, melyek megszüntetik vagy csökkentik a felismert hibák előfordulási valószínűségét és
- a teljes folyamat dokumentálása (ez egy kiegészítő tevékenység annak meghatározására, hogy milyen termék, illetve folyamat teljesíti a vevő igényeit).

Két különböző FMEA csoport pont értékeinek összehasonlítása teljesen helytelen, még akkor is, ha ugyanara a termékre vagy folyamatra vonatkoznak, mivel az egyes csoportok összetétele és körülményei különbözőek és a pontozás bizonyos mértékig mindig szubjektív. Az elkészült FMEA áttekintése a kitűzött minőségcélok tükrében javasolt.

Utógondozás (Follow up)
A megfelelő javító intézkedések bevezetésének és nyomon követésének fontosságát nem lehet túlhangsúlyozni. A bevezetett intézkedéseket minden érintett területtel közölni kell. Egy bármilyen alaposan végiggondolt és gondosan elkészített FMEA is csak nagyon kis értéket képvisel bevezetett javító, illetve megelőző intézkedések nélkül.

Az FMEA elkészítéséért felelős személy feladata az intézkedések bevezetéséről és hatásosságáról meggyőződni. Az FMEA egy élő dokumentum kell legyen, mindig az aktuális állapotot kell tükröznie, figyelembevéve a legutóbbi rajz és technológiai változatot a vonatkozó legfrissebb intézkedésekkel együtt, beleértve a termelés elindulása utáni eseteket is.

A felelős személynek sok eszköz áll a rendelkezésére, hogy meggyőződjön a bevezetett intézkedések hatásosságáról. Fontosabb ilyen eszközök:

1. A műszaki rajzok, folyamatleírások és munkautasítások átnézése, hogy tartalmazzák-e a javasolt intézkedéseket.
2. A megfelelő dokumentációk jóváhagyása a termékre, folyamatra, munkautasításokra vonatkozóan.
3. A megfelelő termék és folyamat-FMEA-k áttekintése, speciális FMEA alkalmazások, „control plan” átvizsgálások.

12.3. Termékek meghibásodási mód- és hatáselemzése

12.3.1. Bevezetés

A termék-FMEA egy elemző eszköz, amelyet a termék tervezéséért felelős mérnök vagy mérnök csoport alkalmaz annak érdekében, hagy azonosítsa a lehetséges meghibásodásokat azok okaival vagy mechanizmusaival együtt, és ezeket figyelembe vegye a termék végső kialakításánál. A végtermékeket minden hozzájuk tartozó alrendszerrel, alkatrésszel együtt ki kell értékelni. Az FMEA szigorúan véve összegzése mindazon gondolatoknak (beleértve valamennyi alkotórész elemzését, melyek a tapasztalatok alapján elromolhatnak), melyek a termék, alrendszer, alkatrész tervezése során felmerülnek. Ez a szisztematikus megközelítés segít megtartani azt a fegyelmet, amely a normális tervezési folyamat szükséges velejárója, és amelyet a tervező mérnök a munkája során gyakorol.

A termék-FMEA a következőkkel járul hozzá a hibák megelőzéséhez:

- segíti a célok kiértékelését a termék esetében, beleértve a funkcionális követelményeket és a tervezés alternatív lehetőségeit,
- lehetővé teszi a korai konstrukció kiértékelést a gyártás szempontjából, az összeszerelés, a szervizelhetőség és az újrahasznosítás figyelembe vételével,
- növeli annak valószínűségét, hogy a lehetséges meghibásodásokat és azok hatásait a termék, illetve folyamat tervezés fázisában figyelembe vették
- járulékos információt szolgáltat ahhoz, hogy egy hatékony és alapos kiértékelési folyamatot lehessen kialakítani a tervezés, fejlesztés munkafázisaira,
- kialakít egy pontszámokkal jellemezhető sorrendet az egyes meghibásodásokra abból a szempontból, hogy azok hatása milyen mértékű a vevőre és ezzel megalapoz egy prioritási sort a rendszer fejlődéséhez, ami magába foglalja a fejlesztést, kiértékelést, vizsgálatokat és elemzéseket.
- formát szolgáltat a kockázat csökkentő intézkedések nyomon követésére,
- referenciát szolgáltat a jövő számára (például a tanulságok megfogalmazása), hogy elemezni lehessen az értékesítés utáni meghibásodásokat és kialakítható legyen egy kifinomult, magas színvonalú tervezési gyakorlat.

12.3.2. A vevő meghatározása

A „vevő” a termék-FMEA szempontjából nem csak a termék „végfelhasználóját” jelenti. A vevő fogalmába beletartoznak azok a műszaki tervezéseket végző mérnök csoportok is, akik egy olyan magasabb szintű termék tervezésén dolgoznak, amelyik alkalmazza a szóban forgó termékeket, és beletartoznak a termelési folyamatokat, szerviz tevékenységeket végző emberek is.

12.3.3. A csoport munka

A tervezési munka kezdeti fázisában az adott termék tervezéséért felelős mérnök felelőssége, hogy minden érintett területről összehívja azok képviselőit. Ezek a területek lehetnek a következők, természetesen nem kizárva esetleg más területek bevonását is:

- szerelési folyamatok,
- gyártási tevékenységek,
- tervezés,
- vizsgálatok,
- megbízhatósági szakértő,
- alapanyag,
- minőségbiztosítás,
- szerviz és
- szállítók; valamint
- a magasabb szintű termék tervező csoportja.

A csoportnak mintegy katalizátorként kell működnie, hogy ösztönözze az ötletek és elképzelések cseréjét az egyes funkciók között. Lehet, hogy a tervező mérnök gyakorlott a csoport munka és az FMEA-készítés területén, de akkor is javasolt egy FMEA-szakember segítségét igénybe venni.

A termék-FMEA-nak teljesen aktuális dokumentumnak kell lennie, ami a következőket jelenti:

- elkészítését a tervezési koncepció kidolgozása alatt, vagy annak véglegesítése előtt el kell kezdeni,
- folyamatosan naprakészen kell tartani, akár a változások esetében, akár ha új információ lesz elérhető a termék fejlesztés különböző szakaszaiban és
- teljes egészében készen kell lennie, mielőtt a termék műszaki rajzait kiadják a szerszámok megtervezéséhez és elkészítéséhez.

Figyelembe véve, hogy a gyártási és szerelési igények ismertek, a termék-FMEA célja a tervezési célkitűzések megvalósulásának elősegítése, feltételezve azt, hogy a terméket gyártani fogják a tervezési célkitűzések megvalósulása érdekében. Azok a meghibásodások, melyek a gyártás során előfordulhatnak, nem szükségszerűen, de szerepelhetnek a termék-FMEA-ban. Ha a termék-FMEA nem tartalmaz ilyen elemeket, akkor ezek szerepelhetnek a folyamat-FMEA-ban.

A termék-FMEA nem hagyatkozhat a folyamatok felügyeletére, szabályozására a termék lehetséges gyengeségei tekintetében, de figyelembe kell venni a gyártási folyamatok fizikai korlátait, mint például:

- a felületi megmunkálások korlátai,
- szerelési helyközök, szerszámok hozzáférése,

- acél keménységének korlátai,
- tűrésmezők véges volta, folyamat teljesítőképességek.

A termék-FMEA figyelembe veheti még a termék karbantarthatóságának fizikai korlátait és a termék újrahasznosítását is, mint például:

- szerszám hozzáférés,
- diagnosztizálási képességek,
- anyagazonosítási/osztályozási szimbólumok.

12.3.4. A termék-FMEA elkészítése

A termék tervezéséért felelős mérnök számtalan dokumentummal rendelkezhet, amely hasznos lehet az FMEA elkésztésénél. A folyamat egy olyan lista elkészítésével kezdődik, amely felsorolja, hogy mik a termékkel szemben támasztott követelmények, mi az, amit a terméknek „tennie kell" és mi az, amit „nem kell tennie". A vevő követelményeit és/vagy a gyártási, szerelési, szerviz és újrahasznosítási követelményeket egyaránt figyelembe kell venni. Minél jobb egy követelmény definiálása annál könnyebb azonosítani a lehetséges meghibásodási módokat és a megelőző/javító intézkedéseket.

A termék-FMEA elkészítését egy blokk diagrammal kell kezdeni, amely bemutatja az elemezni kívánt termék helyét a rendszerben. Egy ilyen blokk-diagramm bemutathatja az információ, az energia, a folyadék áramlást vagy a fellépő erőhatásokat. Célja, hogy megértsük azt a folyamatot, amelynek során a termék valamilyen bemenetet átalakít valamilyen kimenetté, tehát ismerjük meg a bemenetet, a funkciót és a kimenetet.

A diagram-forma jól illusztrálja az elemzés során vizsgált egységek között fennálló elsődleges kapcsolatokat és meghatározza az elemzés logikai sorrendjét. Az FMEA elkészítéséhez használt blokk diagramot csatolni kell az elkészült FMEA-hoz.

A mellékletben szereplő ábra bemutat egy elkészült FMEA-vizsgálatot (2. ábra). Az ott szereplő jelölések magyarázata a következő:

1. FMEA száma:
Az FMEA dokumentum számát írjuk be ide a későbbi azonosítás és nyomonkövethetőség érdekében.

2. Rendszer, Alrendszer, vagy Alkatrész megnevezés és száma
Jelöljük meg, hogy az elemzés szintjét és írjuk be a rendszer, alrendszer, alkatrész megnevezését és az azonosítására szolgáló számot. Az FMEA

csoport tagjainak el kell dönteni, hogy mi alkot rendszer, alrendszert, vagy mi az alkatrész a csoport specifikus tevékenysége szempontjából. A határok meghúzása a rendszer, alrendszer vagy alkatrész szempontjából önkényes és az adott esetben ez mindig a csoport döntésén múlik.

A rendszer FMEA tárgyköre:
A rendszer úgy tekinthető, mint több különböző alrendszerből felépített egység. ezeket az alrendszereket az esetek többségében különböző csoportok tervezik. Tipikus példák arra, amit rendszer FMEA-val lehet lefedni: szerelt műszerfal, erőátviteli rendszer, kocsi belső tér stb.. Ebből következően a rendszer FMEA-nak a rendszert alkotó egyes alrendszerek közötti kapcsolatra kell összpontosítania, valamint a más, a jármű részét alkotó rendszerek és a vevő felé meglévő kapcsolódásokra.

Alrendszer FMEA tárgyköre:
Az alrendszer FMEA általában egy nagyobb rendszer alkotóelemével foglalkozik. Erre példa lehet a szerelt műszerfal rögzítésére szolgáló szerkezeti elem mint alrendszer. Ebből következik, hogy az alrendszer FMEA az alrendszerek egymás közötti kapcsolatára és a rendszerhez való kölcsönhatásra összpontosít, valamint az alrendszer alkotó alkatrészek alrendszerhez való viszonyára.

Alkatrész FMEA tárgyköre:
Az alkatrész FMEA egy alrendszer egy elemére összpontosít. Erre lehet egy példa egy rögzítő elem a műszerfal rögzítésére szolgáló alrendszeren belül.

3. Tervező
Az elemzett egység tervezéséért felelős személy, osztály vagy csoport megnevezése. Ha alkalmas, akkor tüntessük fel a szállító nevét.

4. Készítette
Az FMEA elkészítéséért felelős személy neve, telefonszáma, az érdekelt szervezeti egység (osztály, vállalat) megnevezése.

5. Modell év/Program
Az elemzett egység elhatározott felhasználási területe, illetve modell éve írandó ide, ha ismert.

6. Kiadás dátuma
Az FMEA első esedékességének, kiadásának dátuma, ami nem lehet későbbi mint a termék kibocsátási, jóváhagyási dátuma.

7. FMEA dátuma
Az FMEA első komplett megvalósításának és a legutóbbi felülvizsgálatának dátuma.

8. Alap csoport
Azon csoporttagok nevének felsorolása, akik hatáskörrel és felelősséggel rendelkeznek a feladat azonosítására és végrehajtására.

9. Egység/funkció
Írjuk be az egység nevét és egyéb vonatkozó információkat (például rajzszám, alkatrész osztálya). azt a szóhasználatot alkalmazzuk, ami a műszaki rajzo(ko)n szerepel. A termék első felszabadítása előtt fel kell tüntetni a kísérleti fázisok számának azonosítását.

Amennyire lehet legyünk konzisztensek a funkció megfogalmazásában az elemzett egységet illetően, hogy a termék céljának mindjobban megfeleljünk. alkalmazzunk számszerűsített, mérhető információkat, arra a környezetre, amelyben a terméknek funkcionálnia kell (hőmérsékleti tartomány, nyomás, páratartalom, élettartam). Ha az egység több funkcióval rendelkezik különböző lehetséges meghibásodási módokkal, soroljuk fel mindegyik funkciót.

10. Lehetséges meghibásodási mód
A lehetséges meghibásodás módjának meghatározása, oly módon, hogy leírja az adott rendszer, alrendszer, alkatrész esetében potenciálisan hogyan hiúsulhat meg a tervezett funkció, ami a le van írva az egység/funkció oszlopban (a tervezett funkció nem valósul meg). Az itt leírt potenciális meghibásodás egy potenciális meghibásodási ok lesz a magasabb szintű alrendszer vagy rendszer esetében és hiba hatásaként jelentkezik egy alacsonyabb szintű elem esetében.

Soroljunk fel minden lehetséges meghibásodási módot az adott funkcióval, illetve egységgel kapcsolatban. A feltételezés az, hogy a hiba előfordulhat, de nem biztos, hogy elő is fordul. Egy javasolt kiindulási pont a korábbi tapasztalatok alapján áttekinteni, hogy milyen meghibásodások fordultak elő a korábban és alkalmazni az ötlet-roham technikát a lehetséges meghibásodások azonosítására.

Figyelembe kell venni azokat a lehetséges meghibásodási módokat is, amelyek csak bizonyos körülmények között (alacsony vagy magas hőmérséklet, szárazság, por stb.) vagy sajátos alkalmazás mellett (átlagosnál gyakoribb használat, gépjármű üzemelése csak városi környezetben, nehéz terep) fordulhatnak elő.

Tipikus meghibásodások lehetnek a következők (de nem csak ezek):

- Repedés
- Meglazulás
- Ragadás
- Törés
- Csúszás (pl kuplung)
- Elégtelen tartás (szerkezetileg)
- Kiengedés túl gyors
- Időszakos/bizonytalan jelzés
- Deformálódás
- Szivárgás, folyás
- Korrózió, oxidáció
- Nincs nyomaték átvitel
- Nem tart (szerkezetileg)
- Túl szoros illeszkedés
- Nem megfelelő jelzés
- Nincs jelzés

Megjegyzés: A lehetséges meghibásodások megfogalmazására „fizika", technikai terminológiát alkalmazzunk és ne a tünetek leírását, ahogy ezt esetleg a vevő megfogalmazza.

11. A meghibásodás lehetséges hatása(i)

A funkció meghiúsulásából származó meghibásodás lehetséges hatásait tartalmazza ez az oszlop, ahogy a vevő a hibát érzékeli.

A meghibásodás hatását olyan kifejezésekkel, terminológiával fogalmazzuk meg, ahogy ezt a vevő érzékeli, tapasztalja, emlékezve arra, hogy a vevő lehet belső vevő is ugyanúgy mint a végfelhasználó. Ha a meghibásodás befolyásolhatja a biztonságot, vagy törvények, rendeletek követelményeinek való megfelelést, azt világosan meg kell fogalmazni. A hatásokat mindig az elemzett rendszer, alrendszer, alkatrész szempontjából kell megfogalmazni. Emlékezzünk arra, hogy egy hierarchikus kapcsolat van a rendszer, alrendszerek, alkatrészek között. Egy példa, egy alkatrész törése azt eredményezheti, hogy a jármű rázkódik. Ez a rázkódás eredményezheti egy funkció bizonytalan megvalósulását, ami a vevő elégedetlenségéhez vezethet. A cél az, hogy a lehetséges meghibásodások előrejelzése megtörténjen, a csoport ismereteinek megfelelően.

Tipikus hiba hatások lehetnek a következők (de nem csak ezek):

- Zaj — Durva megmunkálás
- Szabálytalan működés — Nem működik
- Esztétikai probléma — Kellemetlen szag
- Stabilitás hiánya — Elégtelen működés
- Melegedés — Folyás, szivárgás
- Rendszeres működési hiba

12. Hiba hatásának súlyossága

A súlyosság egy adott hiba esetében a legsúlyosabb hatás számmal történő osztályozása. A súlyosság egy relatív értékelés az adott FMEA-n belül. A súlyosság kiértékelésére adott osztályzat csak a termék konstrukciójának megváltoztatásával lehetséges. A súlyosság osztályozására a 12-1. táblázat tartalmaz irányelveket.

Javasolt kiértékelési szempontok:

A csoportnak egyetértésre kell jutnia a kiértékelési szempontokat illetően és ezt konzisztens módon kell alkalmazni, akkor is, még akkor is, ha eltér a szokásostól egyedi termék elemzésére alkalmazzák.

Megjegyzés: A 9 és 10 osztályzathoz tartozó szempontokat nem javasolt módosítani. Ha egy hiba hatásra az értékelés 1, akkor arra a hibahatásra nem kell további elemzést végezni.

Megjegyzés: Magas osztályzatok esetén a hiba hatásának súlya kompenzálható vagy csökkenthető a termék konstrukciójának felülvizsgálatával. Például az ún. „durrdefekt" hatása csökkenthető azzal, ha a gumi lassan ereszt csak le, vagy a biztonsági öv alkalmazása csökkenti a jármű ütközése során fellépő hatás súlyosságát.

13. Osztályozás

Ez az oszlop használható arra, hogy osztályozzuk a speciális termék jellemzőket (például kritikus, alapvető fontosságú, szignifikáns, meghatározó stb.) alkatrészekre, alrendszerekre és rendszerekre, vagy azokra a rendszerekre ahol járulékos tervezési intézkedésekre lehet szükség.

Ez az oszlop annak jelölésére is alkalmas, ha fel akarjuk hívni a figyelmet egy problémára, egy fontos meghibásodási lehetőségre a műszaki kiértékeléshez, vagy a csoport úgy találja, hogy ez segítséget nyújt a további munkához, vagy a helyi vezetés ezt igényli.

Hatás	Kiértékelési szempont a hatás súlyossága	Pontszám
Veszélyes figyelmeztető jel nélkül	Nagyon súlyos következményekkel járó hiba figyelmeztető jelzés nélkül, amely hatással lehet a jármű biztonságos működésére és/vagy magába foglalhat törvényes előírásoknak, rendeleteknek való nem-megfelelést.	10
Veszélyes figyelmeztető jelzéssel	Nagyon súlyos következményekkel járó hiba figyelmeztető jelzéssel, amely hatással lehet a jármű biztonságos működésére és/vagy magába foglalhat törvényes előírásoknak, rendeleteknek való nem-megfelelést.	9
Nagyon magas	Nem működő jármű vagy egység (Valamelyik alapvető funkció nem működik).	8
Magas	A jármű/egység működik de a funkció teljesülési foka alacsony. A vevő nagymértékben elégedetlen.	7
Mérsékelt	A jármű/egység működik, de a kényelmi vagy komfort funkció nem működik. A vevő elégedetlen.	6
Alacsony	A jármű/egység működik, de a kényelmi vagy komfort funkció alacsony szinten működik. A vevő bizonyos mértékig elégedetlen.	5
Nagyon alacsony	Illeszkedési, kikészítési problémák; zörgés, nyikorgás nem elfogadható mértékben. A hibát a vevők többsége (több mint 75%) észreveszi és szóvá teszi.	4
Jelentéktelen	Illeszkedési, kikészítési problémák; zörgés, nyikorgás nem elfogadható mértékben. A hibát a vevők több, mint 50%-a észreveszi és szóvá teszi.	3
Nagyon jelentéktelen	Illeszkedési, kikészítési problémák; zörgés, nyikorgás nem elfogadható mértékben. A hibát a vevők kevesebb, mint 25%-a veszi észre és teszi szóvá.	2
Nincs	A hibának nincs érzékelhető hatása	1

12-1. táblázat: A hibahatás súlyosságának kiértékelési szempontjai termék-FMEA esetén

A speciális termék és folyamat jellemzők azonosítására szolgáló szimbólumokat és azok használatát az egyes vállalatoknak kell meghatározni és erre vonatkozó egységes előírások nem találhatóak ebben a dokumentumban.

14. Hiba lehetséges oka(i)

A hiba lehetséges oka valamilyen tervezési gyengeséget jelent, amelynek egy meghibásodás lehet a következménye.

Soroljunk fel a lehetőségek által megengedett módon minden lehetséges hiba okot minden egyes meghibásodási módhoz. Ennél a lépésnél legyünk következetesek és teljes körűek, amennyire csak lehetséges, annak érdekében, hogy minél hatásosabb javító intézkedéseket alkalmazhassunk.

Tipikus hiba okok lehetnek a következők (de nem csak ezek):

- Nem korrekt anyagspecifikáció
- Nem megfelelő termékélettartam becslés
- Túlzott igénybevétel
- Nem megfelelő kenési képesség
- Nem megfelelő karbantartási utasítások
- Nem megfelelő software specifikáció
- Nem megfelelő erőátviteli specifikáció
- Nem megfelelően specifikált súrlódó anyag
- Túlzott melegedés
- Nem megfelelően specifikált tűrésmező

Tipikus mechanizmusok, a következők lehetek (de nem csak ezek)

- Szakadás, törés
- Anyag kifáradása
- Anyag instabilitás
- Kopás
- Kémiai oxidáció
- Elektronvándorlás
- Elcsúszás
- Korrózió

15. Gyakoriság

A gyakoriság azt a valószínűséget fejezi ki, hogy egy megadott hibaok vagy ~mechanizmus előfordul a termék életében. Az itt adott pontszám egy relatív jelentéssel bír és nem egy abszolút érték. Egy hiba ok vagy mechanizmus kezelésének egyetlen módja a termék konstrukciójának módosítása (konstrukciós ellenőrző lista, konstrukció felülvizsgálata) és így érhető el az előfordulás valószínűségének csökkenése. (A hiba-előfordulás gyakoriságának kiértékelési szempontjait a 12-2. táblázat mutatja be)

Hiba előfordulás valószínűsége	Lehetséges meghibásodási arányszám	Pontszám
Nagyon magas: Állandó jelleggel jelen lévő hiba	hibák száma ≥100db ezer járműre vagy egységre vetítve	10
	hibák száma 50 db ezer járműre vagy egységre vetítve	9
Magas: Gyakori hiba	hibák száma 20 db ezer járműre vagy egységre vetítve	8
	hibák száma 10 db ezer járműre vagy egységre vetítve	7
Mérsékelt: esetlegesen előforduló hiba	hibák száma 5db ezer járműre vagy egységre vetítve	6
	hibák száma 2 db ezer járműre vagy egységre vetítve	5
	hibák száma 1 db ezer járműre vagy egységre vetítve	4
Alacsony: viszonylag kevés hiba	hibák száma 0,5 db ezer járműre vagy egységre vetítve	3
	hibák száma 0,1 db ezer járműre vagy egységre vetítve	2
Elhanyagolható: a hiba előfordulása nem valószínű	hibák száma ≤ 0,010 db ezer járműre vagy egységre vetítve	1

12-2. táblázat: A hiba előfordulási gyakoriságának kiértékelési szempontjai termék-FMEA esetén

A hiba ok vagy mechanizmus előfordulási gyakoriságán becslése egy 1-10 skálán történik. Ennek a kiértékelésnek az elvégzéséhez javasolt a következő kérdések áttekintése:

- Milyen értékesítés utáni szerviz és használati tapasztalatok állnak rendelkezésünkre hasonló termékre?
- A jelenlegi alkatrész régi vagy hasonló egy régi alkatrészhez?
- Milyen jelentős változások vannak egy korábbi termékhez képest?
- Az új alkatrész radikálisan eltér-e a korábban alkalmazottól?
- Az alkatrész teljesen új?
- Az alkatrész alkalmazása megváltozott-e?
- Vannak-e környezeti változások? Ha igen, mik azok?
- Végeztek-e műszaki vizsgálatokat (például megbízhatóság), hogy felmérjék a várható hiba előfordulási valószínűséget?
- Léptettek-e életbe a hiba előfordulását megelőző intézkedéseket?

A gyakoriság kiértékelésénél következetesnek kell lenni a teljes elemzés folyamán. Az itt adott pontszám egy relatív szám az adott FMEA elemzésen belül és nem tükrözi a hiba előfordulás valószínűségének aktuális értékét.

Javasolt kiértékelési szempontok:
A csoportnak egyetértésre kell jutni a kiértékelési szempontokat illetően és legyen a kiértékelés konzisztens, következetes, még akkor is, ha az adott konkrét elemzéshez módosított formában alkalmazzák őket. A 3. táblázat irányelveket tartalmaz a gyakoriság kiértékeléséhez, amelyek alkalmazása javasolt.

Megjegyzés: Az 1 pontszám az „elhanyagolható: a hiba előfordulása nem valószínű" esetre van fenntartva

16. Jelenlegi szabályozás
Soroljuk fel azokat a kiértékelési, felülvizsgálati eljárásokat (validálás, verifikálás) vagy egyéb tevékenységeket, amelyeket annak érdekében végeznek, hogy biztosítsák az adott hiba és hiba ok vagy mechanizmus előfordulásának megelőzését. A jelenlegi ellenőrzések, kiértékelések (tervezés felülvizsgálata, meghibásodás megelőzése, biztonság – például túlnyomásra kiolvadó szelep útján, vizsgálatok, matematikai elemzések, gyárthatóság kiértékelés, prototípus vizsgálatok, országúti vizsgálatok stb.) azok az intézkedések,

melyeket hasonló termékek esetében jelenleg alkalmaznak. A csoportnak mindig törekednie kell arra, hogy a jelenleginél hatékonyabb módszereket azonosítsanak, mint például új labor vizsgálat, új modellező algoritmus stb.

Két fajta szabályozás van a termékre vonatkozóan, amit figyelembe kell venni:

- *Megelőzés:* A törekvés az, hogy megelőzze a meghibásodás előfordulását, vagy csökkentse annak gyakoriságát.
- *Ellenőrzés:* észleli a hiba-ok vagy ~mechanizmus előfordulását, akár elemzési, akár fizikai módszerekkel, mielőtt a terméket felszabadítanák.

Az előnyben részesített megoldás a megelőzés alkalmazása, ha lehetséges. Az elsődleges értékelés a megelőzési intézkedéseken alapul, mint a termék tervezés alapvető szándéka. A detektálásra vonatkozó elsődleges értékelés azon a módszeren alapul, amely a hiba módját vagy a hiba okát, illetve mechanizmusát észleli.

A termék-FMEA formátum ebben a kézikönyvben két oszlopot tartalmaz a jelenlegi szabályozás számára. (külön oszlop a megelőző és külön oszlop a detektáló intézkedésekre), hogy segítse a csoport munkáját, annak tisztázására, hogy egy adott intézkedés milyen jellegű. Ez egyben egy gyors vizuális ellenőrzést is lehetővé tesz, hogy az elemzés során mind a két szempontot figyelembe vették.

Megjegyzés: A jelenleg bemutatott példában első ránézésre látszik, hogy a csoport nem azonosított semmilyen megelőző intézkedést. Ez azt jelezheti, hogy jelenleg hasonló termékekre nem használnak a tervezésnél megelőző megoldást.

Ha olyan formátumot alkalmazunk, ahol csak egy oszlop szerepel erre a célra, akkor a követendő alapelv a következő: Írjunk egy „P” betűt minden felsorolt megelőző (preventív) intézkedés elé. Ugyanígy alkalmazzunk egy „D” betűt a detektáló intézkedések elé.

Ha a jelenlegi szabályozás intézkedéseit felsoroltuk, az előfordulási gyakoriság pontszámait felül kell vizsgálni.

17. Detektálás

A detektálás egy 1-10 skálán végzett osztályozás, ami a legjobb felsorolt detektálási módszer hatásosságát tükrözi (a kiértékelési szempontokat a 12-3. táblázat tartalmazza). A detektálás pontszáma egy relatív szám és csak az adott FMEA-n belül érvényes. Az adott pontszám csökkentése

érdekében hatásosabb megelőzési, ellenőrzési, detektálási (például validálási és verifikálási tevékenységek) módszereket kell bevezetni.

Javasolt kiértékelési szempontok

A csoportnak egyetértésre kell jutnia a kiértékelési szempontokban, amit konzisztens módom kell alkalmazni, még akkor is, ha az adott elemzés során módosították is őket.

Az egyes hibák detektálására szolgáló intézkedések a lehető leghamarabb életbe kell léptetni a fejlesztési munka során.

Megjegyzés: Miután befejeződött a detektálási módszerek kiértékelése, felül kel vizsgálni az előfordulási gyakoriságok pontszámait, hogy azok még mindig helytállóak.
Megjegyzés: Az 1 pontszám fenn van tartva a „szinte teljesen bizonyos” értékelésére.

18. Kockázati tényező (RPN)

A kockázati tényező az eddig megállapított, egymástól független kockázati tényezőkből – a súlyosság (S), a gyakoriság (Gy) és a detektálás (D) – határozható meg:

$$RPN = (S) * (Gy) * (D)$$

Ez az érték az adott FMEA-n belül 1 és 1000 közötti értéket vehet fel és segítségünkre van a termék konstrukciójával kapcsolatos kockázatok mértékének a becslésében.

19. Javasolt intézkedés(ek)

Műszaki kiértékelés, hogy milyen megelőző vagy javító intézkedéseket javasolt életbe léptetni és ezeket elsősorban a nagy súlyú és nagy RPN értékkel rendelkező meghibásodásokra kell alkalmazni, vagy azokra, amelyeket a csoport meghatároz. Minden javító intézkedésnek az a célja, hogy csökkentse a meglévő kockázatokat a következő sorrendben: a hiba hatásának súlya, az előfordulás gyakorisága, a detektálás hatásossága.

Az általános gyakorlat az, hogy ha a hiba hatásának súlya 9 vagy 10, akkor, olyan speciális javító/megelőző intézkedést kell megfogalmazni, amely az adott kockázatra irányulnak, függetlenül az RPN értékétől. Minden olyan esetben amikor az azonosított hiba hatása veszélyt jelenthet a végfelhasználóra, akkor a javító/megelőző intézkedéseket kell alkalmazni a következmények elkerülése érdekében a hiba okok megszüntetésével, csökkentésével vagy ellenőrzésével.

Detektálás	Kiértékelési szempont: a detektálás valószínűsége	Pontszám
Teljesen bizonytalan	A jelenlegi megoldás nem fogja vagy nem tudja detektálni az adott meghibásodást, annak okát vagy nincs is ilyen intézkedés.	10
Nagymértékben elhanyagolható	Nagymértékben elhanyagolható annak a valószínűsége, hogy az alkalmazott módszer detektálja az adott meghibásodást.	9
Elhanyagolható	Elhanyagolható mértékben valószínű, hogy az alkalmazott módszer detektálja az adott hibát.	8
Nagyon alacsony	Nagyon alacsony a valószínűsége annak, hogy a módszerrel az adott hiba vagy annak oka detektálható.	7
Alacsony	Alacsony a valósínűsége, hogy az alkalmazott módszer az adott hibát vagy annak okát detektálja.	6
Mérsékelt	Mérsékelten valószínű, hogy az alkalmazott módszer az adott hibát vagy annak okát detektálja.	5
Mérsékelten magas	Mérsékelten magas a valósínűsége, hogy az alkalmazott módszer az adott hibát vagy annak okát detektálja.	4
Magas	Magas a valósínűsége, hogy az alkalmazott módszer az adott hibát vagy annak okát detektálja.	3
Nagyon magas	Nagyon magas a valósínűsége, hogy az alkalmazott módszer az adott hibát vagy annak okát detektálja.	2
Szinte teljesen bizonyos	Az alkalmazott módszer nagy bizonyossággal detektálja az adott hibát vagy annak okát.	1

12-3. táblázat: A hibaelőfordulás detektálásának kiértékelési szempontjai termék-FMEA esetén

Miután speciális intézkedéseket vezettek be a súlyos hatású kockázatokra, 9–10 értékek, a csoport a többi meghibásodásra fogalmaz meg javító intézkedéseket a súlyosság, előfordulási gyakoriság csökkentésére, illetve a detektálás hatásosságának növelésére.

A javító intézkedések meghatározásánál a következők (de nem csak ezek) vehetők figyelembe:

- A termék geometriájának, méreteinek és a hozzájuk tartozó tűrések felülvizsgálata,
- Az anyag specifikáció felülvizsgálata,
- DOE (Design Of Experiments – Kísérletek tervezése) ha több tényező együttes hatásával kell számolni, vagy más probléma megoldó módszerek alkalmazása és
- A vizsgálati módszerek és tervek felülvizsgálata.

A javasolt intézkedések elsődleges célja, hogy csökkentsék a kockázatokat és növeljék a vevő megelégedettségét a termék konstrukciójának, kialakításának javításával.

A meghibásodás hatásának súlya csak a termék módosításával lehetséges. A hiba előfordulásának gyakorisága csak az okok vagy mechanizmusok egy részének megszüntetésével érhető el. A termék kiértékelési tevékenységek (verifikálás, validálás) hatásosságának javításával érhető el a detektálási pontszám javítása. A kiértékelési tevékenységek javítása a legkevésbé hasznos, mert nem csökkenti a hiba hatásának súlyát vagy az előfordulás gyakoriságát.

Ha egy kockázat esetében a csoport úgy ítéli meg, hogy nem szükséges javító intézkedés, akkor ezt jelöljük például NA (Nem Alkalmazandó) bejegyzéssel.

20. Felelős/határidő

Ebbe az oszlopba írjuk be az intézkedés bevezetéséért felelős személy vagy szervezet nevét és a tervezett határidőt.

21. Bevezetett intézkedés

Miután az intézkedést bevezették, ebbe az oszlopba írjuk be röviden megfogalmazva a hatályba lépés dátumával.

22. Eredmény

A meghatározott és bevezetett intézkedés kiértékelését is el kell végeznünk a hiba hatás súlyossága, az előfordulás gyakorisága és a detektálás hatásos-

sága szempontjából. Ezután meghatározhatjuk a kockázati tényezőt (RPN). Ha nem volt javasolt intézkedés, akkor hagyjuk ezeket az oszlopokat üresen.

Minden felülvizsgált intézkedést nézzünk át újra, ha szükséges végezzük el újra az elemzést. Mindig a folytonos fejlődésre összpontosítsunk.

Nyomonkövetés

A tervezésért felelős mérnök felelőssége, hogy a meghatározott intézkedések bevezetéséről és azok hatásosságáról meggyőződjön. Az FMEA egy élő dokumentum kell, hogy legyen, ami azt jelenti, hogy mindig a legutolsó tervezési változatot, bevezetett intézkedést kell tükröznie, beleértve a sorozatgyártás felszabadítása utáni módosításokat.

A tervezésért felelős mérnöknek számtalan lehetőség áll rendelkezésére, hogy meggyőződhessen az intézkedések bevezetéséről. Ezek (és nem csak ezek) a következők lehetnek:

- meggyőződik arról, hogy a termékkel szemben támasztott követelmények teljesülnek,
- átnézi a kiadott rajzokat és specifikációkat,
- átnézi a vonatkozó szerelési/gyártási utasításokat,
- átnézi a folyamat-FMEA-t és „control Plan”-t.

12.4. Folyamatok meghibásodási mód és hatás elemzése

12.4.1. Bevezetés

A folyamat-FMEA teljesen a termék-FMEA módján definiálható (a 12.3.1 fejezetben mondottakat értelemszerűen alkalmazva a folyamatra). A folyamat-FMEA :

- azonosítja a folyamattal szemben támasztott követelményeket,
- azonosítja a lehetséges termék- és folyamatvonatkozású meghibásodási módokat,
- kiértékeli a lehetséges meghibásodások vevőkre gyakorolt hatását,
- azonosítja a meghibásodások okait a gyártó/szerelési folyamatokban, valamint azokat a folyamatjellemzőket, melyek szabályozásával elérhető a kimeneten jelentkező meghibásodások számának csökkenése vagy javítható a hiba detektálásának hatásossága,

- azonosítja azokat a folyamat-jellemzőket, melyek szabályozására nagy figyelmet kell szentelni,
- felállít egy kockázati tényezővel rendelkező listát a lehetséges meghibásodási módokról, amelynek segítségével meghatározható egy prioritási sorrend a javító/megelőző intézkedések számára,
- dokumentálja a gyártási/szerelési folyamatra bevezetett intézkedések eredményét.

12.4.2. A vevő meghatározása

A „vevő" a termék-FMEA szempontjából általában a termék „végfelhasználóját" jelenti. Azonban a folyamat-FMEA esetében minden soron következő folyamat vagy művelet is vevőként értelmezendő.

12.4.3. A csoport munka

A folyamat tervezési munka kezdeti fázisában a 12.3.3 fejezetben mondottakkal azonos módon az adott termék tervezéséért felelős mérnök felelőssége, hogy minden érintett területről összehívja azok képviselőit. Ezek a területek a folyamat-FMEA esetén a következők (természetesen nem kizárva esetleg más területek bevonását is):

- termék tervezés,
- fejlesztés,
- szerelési folyamatok,
- gyártási tevékenységek,
- tervezés,
- vizsgálatok,
- megbízhatósági szakértő,
- alapanyag,
- minőségbiztosítás,
- szerviz és szállítók; valamint
- a magasabb szintű szerelvény tervező csoportja.

A folyamat-FMEA aktualitásának biztosítására kidolgozását meg kell kezdeni:

- a gyárthatóság elemzés előtt vagy annak fázisában,
- a gyártás felszerszámozása előtt, és
- minden alkatrész vagy szerelvény gyártási folyamatára el kell végezni.

A korai áttekintés érdekében új vagy felülvizsgált és módosított folyamat esetén a gyártási folyamat tervezésének korai fázisában javasolt a folyamattal kapcsolatos problémák előrejelzése, megoldása, nyomon követése. A folyamat-FMEA feltételezi, hogy a termék a megtervezett módon megfelel a követelményeknek. Azokat a lehetséges meghibásodásokat, melyek a termék valamilyen gyengesége miatt fordulhatnak elő, a folyamat-FMEA-ban kell felderíteni. A termék meghibásodásainak hatásait és azok elkerülésének módjait a termék-FMEA foglalja magába.

A folyamat-FMEA nem a termék módosításaira épít, hogy a folyamat gyengeségeit megoldja, azonban figyelembe veszi azt, hogy ha a termék megfelel a tervezett jellemzőknek, vagy a folyamat előírás szerint működik, akkor a termék megfelel a vevő igényeinek is.

12.4.4. A folyamat-FMEA elkészítése

Az FMEA elkészítése ebben az esetben is egy lista létrehozásával kezdődik, amely tartalmazza, hogy a folyamatnak mit kell megvalósítania és mit nem. E feltételek kidolgozásához számos dokumentáció áll a mérnökök rendelkezésére.

A folyamat-FMEA kidolgozása is egy a folyamatot leíró diagram (folyamat ábra) létrehozásával kezdődik. Ennek a folyamat ábrának tartalmaznia kell minden műveletre a vonatkozó folyamat paramétereket és termék-jellemzőket. Ha rendelkezésre áll a termék-FMEA, akkor annak folyamatvonatkozású elemeit figyelembe kell venni. Az FMEA elkészítéséhez alkalmazott folyamat ábrát az FMEA-hoz mellékelni kell.

A melléklet 3. ábrája mutat egy folyamat-FMEA elkészítésének támogatására készített formanyomtatványt. Az ott szereplő számjelölések magyarázatát a következőkben adjuk meg:

1. FMEA száma
Ide írjuk be az FMEA azonosítására szolgáló számot, amit a nyomon követésre is használunk.

2. Egység/alkatrész
Ide írjuk az elemzett egység (rendszer, alrendszer, alkatrész) megnevezését, számát, amelynek előállítási folyamatát elemezni fogjuk.

3. Folyamat felelősség
Írjuk be a felelős személy szervezet nevét és a szállítót, ha ismert.

4. Készítette
Az FMEA elkészítéséért felelős személy neve, telefonszáma, foglalkoztató szervezete

5. Modell év/program
Az elemzett terméket és folyamatot felhasználó modell vagy program kibocsátási éve, ha ismert.

6. Kiadás dátuma
Ide írjuk be az FMEA kidolgozásának kezdeti dátumát. Ez a dátum nem lehet későbbi, mint a termék és folyamat felszabadításának dátuma.

Megjegyzés: Külső szállító esetében az FMEA dátuma nem lehet későbbi mint a tervezett termék és folyamat jóváhagyási dátum (PPAP submission date)

8. Alap csoport
Azoknak a személyeknek a felsorolása, akik felelősek az FMEA elkészítéséért (Javasolt, hogy a személyek neve mellett tüntessük fel a szervezetüket és telefonszámaikat is).

9. Folyamat funkció/követelmény
Írjuk be ide az elemzett folyamat egyszerű megnevezését (pl, fúrás, esztergálás, marás, hegesztés stb.). Javasolt az elemzett lépés azonosító számát is beírni. A csoportnak figyelembe kell vennie az alkalmazható előírásokat a teljesítményre, anyagra, környezetvédelemre és a biztonságos munkavégzésre vonatkozóan. Amennyire lehet konzisztens módon fel kell tüntetni a célját annak a részfolyamatnak, ami épp az elemzés tárgya, beleértve a termékre vonatkozó információt is (mérhető termékjellemzők). Ahol a folyamat több műveletet tartalmaz (például szerelés) különböző lehetséges meghibásodásokkal, ott ajánlott minden műveletet mint külön elemet feltüntetni.

10. Lehetséges meghibásodás mód
A lehetséges meghibásodás mód úgy határozható meg, hogy a folyamat milyen módon nem teljesíti azt a folyamat vagy termék követelményt, ami a bal oldali oszlopban meg van fogalmazva. Ez egy leírása a nemmegfelelőségnek az adott műveletre vonatkozóan. Ez értelmezhető úgy, mint egy hiba ok valamelyik következő műveletnél, vagy egy hibahatás

valamelyik korábbi műveletre vonatkozóan. Az alapfeltételezés azonban az, hogy az alkatrész a korábbi műveletről korrekt módon érkezik meg. Kivételt akkor érdemes tenni, ha a tapasztalat azt mutatja, hogy előfordulnak meghibásodott alkatrészek a bejövő anyagok között.

Soroljunk fel a lehetőségek keretein belül minden lehetséges meghibásodást az adott műveletre a rendszer, alrendszer, alkatrész, folyamat paraméter vonatkozásában. Tételezzük fel, hogy a hiba előfordulhat, de nem szükségszerűen fordul elő.

A csoportnak fel kell tennie és meg kell válaszolnia a következő kérdéseket:

- Hogyan hiúsíthatja meg a folyamat/termék a követelmények teljesülését?
- Függetlenül a műszaki specifikációtól, mit tekinthet a vevő (végfelhasználó, következő művelet(ek), szerviz) kifogásolhatónak.
- Kezdjük a hasonló folyamatok áttekintésével, a korábbi vevői (végfelhasználó, soron következő művelet) észrevételekkel. ezen kívül fontos még a termék alkalmazási céljának az ismerete. Tipikus meghibásodások lehetnek (de nem csak ezek):

Görbült	Égett	Furat rossz poz.
Repedt	Furat eltömődött	Hiányzó furat
Kezelési sérülés	Piszkos	Furat túl mély
Durva felület	Deformálódott	Felület túl sima
Szakadt áramkör	Rövidzár	Rossz cimkézés

Megjegyzés: A lehetséges meghibásodások megfogalmazásához használjunk fizikai műszaki terminológiát és ne tüneti leírásokat, ahogy ezt a vevő érzékeli.

11. Hiba lehetséges hatása

A meghibásodás hatását úgy határozhatjuk meg, mint a meghibásodás módjának hatása a vevő(k)re.

Úgy írjuk le a hatást, ahogy azt a vevő vagy vevők érzékelhetik, nem megfeledkezve arról, hogy a vevő lehet belső vevő is. Tüntessük fel világosan és egyértelműen, ha a hiba hatása biztonságtechnikai következményekkel vagy törvényes előírások és rendeletek követelményeinek nem teljesülésével jár együtt. Vevő a folyamat-FMEA összefüggéseiben minden

következő művelet, folyamat, felhasználó (például szerviz, dealer, a jármű vásárlója és üzemeltetője). Ezek mindegyikét figyelembe kell vennünk, amikor a hibák lehetséges hatásait értékeljük.

A végfelhasználó számára jelentkező hibát úgy kell megfogalmazni, hogy a termék, folyamat teljesítményét tükrözze, mint például

Zaj	Durva zaj, felület,
Egyenetlen működés	Túlzott például melegedés
Erőlködés (működésben)	Nem működik
Kellemetlen szag	Nem stabil
Akadozó működés	Esztétikai problémák
Szivárgás	Jármű irányíthatóság pr.
Javítás, újra munkálás	Vevői elégedetlenség
Selejt	

Ha a vevő a következő műveletek valamelyike, akkor a hatást a folyamat teljesítése szempontjából kell megfogalmazni, mint például:

Nem rögzíthető	Nem illeszkedik
Nem dugható a helyére	Nem csatlakozik
Nem szerelhető	Nem passzol
Nagymértékű szerszámkopást eredményez	
Kárt okoz a berendezésben	Veszélyt jelent az operátorra

12. Hiba hatásának súlyossága

A hiba hatásának súlyosságát egy pontszámmal értékeljük. Ez az értékelés egy relatív pontszám az adott FMEA-n belül.

Ha a hiba hatását a vevő érzékeli, vagy olyan távoli felhasználó (jármű összeszerelő), akkor a hatás súlyosságának kiértékelése kívül eshet a folyamat-FMEA csoport ismeret körén. Ebben az esetben konzultálni kell a termék tervezéséért felelős műszak szervezetekkel.

Javasolt kiértékelési szempontok

A csoportnak egyetértésre kell jutnia a kiértékelési szempontokat és a pontozást illetően, amit következetesen alkalmazni kel, még akkor is, ha ezeket az adott alkalmazás esetére módosították. (lásd a 12-4. táblázatot)

A hiba hatás súlyosságának kiértékeléséhez a 4. táblázatot mint irányelvet kell alkalmazni.

Megjegyzés: Nem javasolt módosítani a 9 és 10 pontszámhoz tartozó kiértékelési elveket. Az 1 pontszámmal értékelt hatásokat nem kell tovább elemezni.

13. Osztály

Ez az oszlop használható bármilyen speciális termék vagy folyamat jellemző azonosítására (például kritikus, szignifikáns, alapvető fontosságú stb.) alkatrészekre, alrendszerekre vagy rendszerekre, amelyek a folyamat kézbentartása szempontjából további intézkedéseket igényelhetnek.

Ez az oszlop alkalmazható a magas prioritású meghibásodások azonosítására is a további műszaki kiértékelések támogatására.

Ha az osztály oszlopba bejegyzést teszünk, arról értesíteni kell a termék tervezésért felelős mérnököt vagy mérnök csoportot, mert lehet, hogy az osztályozásnak hatása van műszaki és technológiai dokumentációkra.

A speciális jellemzők vagy paraméterek azonosítására szolgáló szimbólumok alkalmazását az érvényes vállalati politikák szerint kell alkalmazni, erre jelen kiadvány nem tartalmaz előírásokat.

14. A meghibásodás lehetséges oka(i), mechanizmusa(i)

A hiba lehetséges okának meghatározása, oly módon, hogy a hibát ez hogy okozhatja, olyan megközelítésben, hogy valami, ami kijavítható vagy ellenőrizhető.

A lehetőségekhez képest soroljunk fel minden hiba okot hozzárendelve minden egyes meghibásodáshoz, például ha az adott hibaok közvetlen hatással rendelkezik a meghibásodás módjára, akkor ez a része az FMEA-nak kész. Sok olyan lehetséges ok van, amelyek nem kölcsönösen kizárólagosak, ilyenkor például a DOE módszer alkalmazásával lehet azokat az okokat azonosítani, melyek leginkább hozzájárulnak a meghibásodás létrejöttéhez és amelyek a leginkább kézbentarthatóak. Az okokat úgy kell leírni, hogy javító intézkedések legyenek meghatározhatóak az egyes okokra vonatkozóan. Tipikus kiváltó okok lehetnek (de nem csak ezek):

- Nem előírt nyomaték – magasabb, alacsonyabb
- Nem megfelelő hegesztés – áramerősség, idő, nyomás
- Nem pontos mérés
- Nem megfelelő hőkezelés – idő, hőmérséklet
- Nem megfelelő nyílás/szellőzés

Hatás	**Szempont: a hatás súlya** Ez az értékelés arra az esetre szól, ha a hiba hatása a végfelhasználónál vagy a jármű összeszerelő üzemben jelentkezik. Mindig a végfelhasználót kell először figyelembe venni. Ha mindkettő előfordul, akkor a súlyosabb hatás veendő figyelembe. (**Hatás a vevőnél)**	**Szempont: a hatás súlya** Ez az értékelés arra az esetre szól, ha a hiba hatása valamelyik következő folyamatnál, műveletnél jelentkezik. Ha több helyen jelentkezhet a hatás, akkor a legsúlyosabbat kell figyelembe venni. **(Hatás a gyártásra, szerelésre)**	Pont-szám
Veszélyes figyelmeztető jelzés nélkül	Nagyon súlyos hatás, amikor a meghibásodás eredménye a jármű biztonságos működését befolyásolja, illetve törvény vagy rendelet követelménye hiúsul meg, figyelmeztető jelzés nélkül.	Vagy veszélyt jelent az operátorra (gépkezelő, szerelő munkás) figyelmeztető jelzés nélkül.	10
Veszélyes figyelmeztető jelzéssel	Nagyon súlyos hatás, amikor a meghibásodás eredménye a jármű biztonságos működését befolyásolja, illetve törvény vagy rendelet követelménye hiúsul meg, figyelmeztető jelzéssel	Vagy veszélyt jelent az operátorra (gépkezelő, szerelő munkás) figyelmeztető jelzéssel.	9
Nagyon magas	A jármű/egység nem működik (nem valósul meg az elsődleges funkció),	Vagy a termékek 100%-a leselejtezésre kerül, vagy a termék/egység javítására szakműhelyben több mint 1 órát kell szánni.	8
Magas	A jármű/egység működik de a funkció teljesülési foka alacsony. A vevő nagymértékben elégedetlen.	Vagy a terméket válogatni kell (kevesebb mint 100% leselejtezése) vagy a termék javítására szakműhelyben 0,5 – 1 óra javítási idő szükséges.	7
Mérsékelt	A jármű/egység működik, de a kényelmi vagy komfort funkció nem működik. A vevő elégedetlen.	Vagy a termék leselejtezése (kisebb mint 100%-ban) válogatási szükségszerűség nélkül, vagy a szakműhelyben történő javítás időigénye kevesebb mint fél óra.	6
Alacsony	A jármű/egység működik, de a kényelmi vagy komfort funkció alacsony szinten működik. A vevő bizonyos mértékig elégedetlen.	Vagy a termék 100%-a átmunkálandó, vagy a jármű, szerelvény javítása, de ez a gyártás helyén megoldható, nem kell javító helyre vinni.	5
Nagyon ala-	Illeszkedési, kikészítési problémák; zörgés, nyikorgás	Vagy a termék válogatásra szorulhat, nem kell selejtezni és a	4

Hatás	**Szempont: a hatás súlya** Ez az értékelés arra az esetre szól, ha a hiba hatása a végfelhasználónál vagy a jármű összeszerelő üzemben jelentkezik. Mindig a végfelhasználót kell először figyelembe venni. Ha mindkettő előfordul, akkor a súlyosabb hatás veendő figyelembe. (**Hatás a vevőnél)**	**Szempont: a hatás súlya** Ez az értékelés arra az esetre szól, ha a hiba hatása valamelyik következő folyamatnál, műveletnél jelentkezik. Ha több helyen jelentkezhet a hatás, akkor a legsúlyosabbat kell figyelembe venni. **(Hatás a gyártásra, szerelésre)**	Pont-szám
csony	nem elfogadható mértékben. A hibát a vevők többsége (több mint 75%) észreveszi és szóvá teszi.	teljes mennyiséget átmunkálni.	
Jelentéktelen	Illeszkedési, kikészítési problémák; zörgés, nyikorgás nem elfogadható mértékben. A hibát a vevők több mint 50%-a észreveszi és szóvá teszi.	Vagy, a termékek egy része esetleg átmunkálásra, javításra szorul és nem kell selejtezni, a javítás a gyártó helyen végezhető, de nem a művelet helyszínén	3
Nagyon jelen-téktelen	Illeszkedési, kikészítési problémák; zörgés, nyikorgás nem elfogadható mértékben. A hibát a vevők kevesebb, mint 25%-a veszi észre és teszi szóvá.	Vagy, a termékek egy része esetleg átmunkálásra, javításra szorul és nem kell selejtezni, a javítás a gyártó helyen végezhető, művelet helyszínén.	2
Nincs	A hibának nincs érzékelhető hatása	Vagy apró kényelmetlenség a műveleten az operátor számára, vagy nincs hatás.	1

12-4. táblázat: A hibahatás súlyosságának kiértékelési szempontjai folyamat-FMEA esetén

- Nem megfelelő kenés
- Hiányzó, rosszul rögzített alkatrész
- Kopott tájoló
- Kopott szerszám
- Forgács a tájolón
- Törött szerszám
- Helytelen gép beállítás
- Helytelen programozás

Csak a specifikus hibák vagy hibás funkciók rögzítendők, nem egyértelmű kifejezéseket (például operátor hiba, géphiba) ne használjunk.

15. Az előfordulás gyakorisága

Az előfordulás valószínűsége annak a valószínűségét fejezi ki, hogy egy adott specifikus ok előfordul. A gyakoriság értékelése egy relatív érték és nem egy abszolút szám. A hibák megelőzése vagy felismerése a két lehetséges mód a gyakoriság mérőszámának csökkentésére.

A előfordulás gyakoriságát egy 1-10 skálán értékeljük ki. Az értékelésnél a következetességet szem előtt kell tartani. Egy megadott FMEA-n belül ez a szám egy relatív szám és nem biztos, hogy az adott hiba előfordulási valószínűségét kifejező aktuális érték.

A „lehetséges hiba gyakoriság" a folyamat végrehajtása során várható hibák számán alapul. Ha hasonló folyamatokról vannak statisztikai adataink, akkor használjuk ezeket a kiértékelés során. Minden egyéb esetben egy szubjektív kiértékelést végezhetünk az előző oszlopban lévő szóbeli meghatározás valamint a korábbi tapasztalatok alapján.

Javasolt kiértékelési szempontok

A csoportnak egyetértésre kell jutnia a kiértékelési kritériumokat illetően, még akkor is, ha ezeket az adott alkalmazás esetén módosítják. Az előfordulás gyakoriságának kiértékeléséhez mint irányelvet a 12-5. táblázatot kell alkalmazni.

Megjegyzés: Az 1 pontszám az „elhanyagolható, a hiba előfordulása nem valószínű" esetre van fenntartva.

Valószínűség	Valószínűsíthető meghibásodási arány*	Pontszám
Nagyon magas: nagyon gyakori, makacs hiba	≥ 100 hiba ezer darabonként	10
	50 hiba ezer darabonként	9
Magas: Gyakran előforduló hiba	20 hiba ezer darabonként	8
	10 hiba ezer darabonként	7
Jelentős: esetenként előforduló hiba	5 hiba ezer darabonként	6
	2 hiba ezer darabonként	5
	1 hiba ezer darabonként	4
Alacsony: ritkán előforduló hiba	0,5 hiba ezer darabonként	3
	0,1 hiba ezer darabonként	2
Elhanyagolható, nem valószínű	≤ 0,01 hiba ezer darabonként	1

* a kapcsolatos Ppk kalkulációkat itt most nem közöljük

12-5. táblázat: A hiba előfordulási gyakoriságának kiértékelési szempontjai folyamat-FMEA esetén

16. Jelenlegi szabályozás

A jelenlegi szabályozás azokat az intézkedéseket foglalja magába, amelyek egyrészt a hibák előfordulásának megelőzését vagy azok detektálását szolgálja. Ezek az intézkedések lehetnek a folyamat kézbentartását szolgáló intézkedések, mint a tévedés biztos megoldások, SPC, vagy lehetnek a folyamat utáni kiértékelések. Ezek a kiértékelések lehetnek az adott folyamat részei vagy a következő folyamat elemei.

Alapvetően két fajta folyamattal kapcsolatos intézkedést veszünk itt figyelembe:

- *Megelőzés:* A megelőző intézkedések a hiba okát vagy annak kialakulási mechanizmusát előzik meg, vagy az előfordulások gyakoriságát csökkentik.
- *Detektálás:* Detektálja a hibát vagy annak kialakulási mechanizmusát és javító intézkedéshez vezet.

Az előnyben részesített megoldás a megelőzés, ha erre van lehetőség. Az elsődleges kiértékelés a megelőzés alapján történik, ha van, amit a folyamat integrált részének tekintünk. A detektálás értékelése elsősorban a folyamatban meglévő ellenőrzéseken alapul, melyek észlelik a hibát, a hiba okát vagy mechanizmusát.

Ez a kézikönyv a jelenlegi szabályozásra két oszlopot tartalmaz, (egyet a megelőző, egyet a detektáló intézkedésekre), hogy segítséget nyújtson a csoportnak a két fajta megoldás egyértelmű megkülönböztetésére. Ez lehetővé tesz egy gyors, vizuális ellenőrzést arra, hogy mind a két fajta lehetőséget figyelembe vegyük. Ennek a két oszlopos megoldásnak az alkalmazása az amit előnyben részesítünk.

Ha a jelenlegi szabályozásra egy oszlopot alkalmazunk, akkor kövessük a következő alapelvet: A megelőző intézkedésekhez írjunk egy 'P' betűt (Prevention), az ellenőrzési tevékenységekhez egy 'D' (Detection) betűt a vizuális azonosítás céljából.

Ha egy folyamatot kielemeztünk, akkor tekintsük át még egyszer az összes gyakorisági kiértékelést, és ha szükséges, akkor módosítsunk.

17. Detektálás

A detektálás egy kiértékelés, ami a legjobb hatású felsorolt detektáló intézkedést értékeli ki, egy relatív szám segítségével az adott FMEA-n belül. Ahhoz, hogy ezt a számot csökkenteni tudjuk, a tervezett folyamat kézbentartására vonatkozó intézkedéseken kell javítani.

Tételezzük fel, hogy a hiba megtörtént és ezután értékeljük ki a jelenlegi szabályozás hatásosságát. Ezeknek az intézkedéseknek elsősorban az a célja, hogy megakadályozzák a hibás termékek továbbadását a következő folyamathoz. Ne induljunk ki abból, hogy ha a hiba előfordulási gyakorisága alacsony, akkor alacsony értéket adhatunk a detektálásra is (például mert SPC kártyát alkalmazunk), hanem a folyamatnak azt a képességét értékeljük, hogy milyen hatásosan akadályozza meg a hibás termékek továbbadását.

A véletlenszerűen alkalmazott minőség ellenőrzések nagyon alacsony valószínűséggel szűrnek ki egy- egy izolált hibát és nem befolyásolhatják a detektálás kiértékelését. A statisztikai alapon végzett mintavételezés az, ami lehet egy hatékony hiba felderítés.

Javasolt kiértékelési szempontok

A csoportnak egyetértésre kell jutnia a kiértékelési szempontokat illetően, még akkor is, ha azokat az adott FMEA esetére módosították. Az alkalmazás során a következetességre kell törekedni (lásd a 12-6. táblázatot).

Megjegyzés: Az 1 kiértékelési eredményt fenn kell tartani „biztosan detektált” esetre

18. Kockázati tényező RPN

A kockázati tényező (Risk Priority Number) a három tényező, a hatás súlya, az előfordulás gyakorisága, a detektálás hatásossága, szorzata:

$$RPN = (S) * (Gy) * (D)$$

Az adott FMEA-n belül ez a szám értékeli egymáshoz képest az egyes kockázatokat egy 1 – 1000 tartományban

19. Javasolt intézkedések

Műszaki javaslatokat elsősorban megelőző, illetve javító intézkedések formájában azokra az esetekre kell javasolni, ahol magas a hiba hatás súlya, vagy a folyamat kockázata, RPN. A csoport meghatározhat más eseteket is. Minden javasolt intézkedés célja a folyamat kockázatának csökkentése a következő sorrendben: hatás súlya, előfordulás gyakorisága, detektálás hatásossága.

Detektálás	Szempont	Ellenőrzés típusa			Javasolt értékelés a detektálási módszerhez	Pont
		A	B	C		
Szinte lehetetlen	Teljesen biztos, hogy a hibát nem észleli			**X**	Nem lehet észlelni a hibát, vagy nincs is ellenőrzés	10
Nagyon elhanyagolható	Valószínű, hogy a hibát nem detektálja			**X**	Van ellenőrzés, de indirekt vagy véletlenszerű	9
Elhanyagolható	Kicsi a valószínűsége a hiba detektálásának			**X**	A detektálás csak vizuális ellenőrzéssel valósul meg	8
Nagyon alacsony	Nagyon alacsony valószínűséggel detektálja a hibát			**X**	A detektálás csak dupla vizuális ellenőrzéssel valósul meg	7
Alacsony	Lehet, hogy detektálja a hibát		**X**	**X**	A detektálás valamilyen ábrázolási technikával történik, például SPC	6
Mérsékelt	Lehet, hogy detektálja a hibát		**X**		Az ellenőrzés mérhető mennyiség mérésével vagy 100%-os megy-nem megy ellenőrzéssel történik, miután a terméken egy műveletet befejeztek.	5
Mérsékeltnél nagyobb	Jó esély van a hiba detektálására	**X**	**X**		A hiba detektálása egy következő műveletnél történik, VAGY a mérés a gép beállításakor történik az első darabok mérésével (csak beállítással járó esetekre)	4
Magas	Jó esély van a hiba detektálására	**X**	**X**		A hiba detektálása a művelet helyszíné, vagy a következő műveletnél, az elfogadás több lépésében, mint továbbadás, kiválasztás, installálás, igazolás. Nincs lehetőség hibás termék elfogadására.	3
Nagyon magas	Majdnem biztos a hiba detektálása	**X**	**X**		A hiba detektálása a művelet helyszínén (automatikus mérés automatikus megállító rendszerrel). Nem lehetséges hibás darab továbbadása.	2
Nagyon magas	A hiba detektálása biztos	**X**			Nem lehetséges hibás darabok előállítása tévedés-biztos tervezési megoldások miatt.	1

Ellenőrzési típusok: A: Hiba vagy tévedés biztos; B: Mérés; C: Kézi ellenőrzés

12-6. táblázat: A hiba-előfordulás detektálásának kiértékelési szempontjai folyamat-FMEA esetén

Általános gyakorlat, hogy ha hatás súlya 9 vagy 10, akkor különös figyelmet kell szentelni, hogy a javító intézkedés a jelenlegi termék terven keresztül valósuljon meg, függetlenül a másik két tényezőtől. Minden olyan esetben ahol a hiba veszélyt jelent a gyártást végző személyzetre, megelőző vagy javító intézkedést kell életbe léptetni, ami megelőzi a hiba előfordulását vagy a hiba ok megjelenését detektálja és a dolgozó védelmét megfelelően elő kell írni.

Minden 9 vagy 10 értékelés esetén a súlyosságra kell először javító intézkedést megfogalmazni, ezután pedig a magas RPN esetekre a fenti sorrendben.

A javító intézkedések, természetesen nem kizárva egyéb lehetőségeket a következők lehetnek például:

- a hiba előfordulás gyakoriságának csökkentéséhez a folyamat és a termék együttes felülvizsgálata szükséges,
- statisztikai módszerek alkalmazásával tevékenység-orientált tanulmány készítése a folyamatra vonatkozóan, folyamatos információ visszacsatolással a megfelelő fejlődés és a hiba megelőzés érdekében,
- a hiba hatásának súlyosságát csak a termék és/vagy a folyamat felülvizsgálata és módosítása csökkentheti.

Az előnyben részesített módszer a hiba detektálás esetében a tévedésbiztos tervezési megoldások alkalmazása. Általában az ellenőrzés szigorítása költséges megoldás és nem hatékony. Az ellenőrzések gyakoriságának növelése nem hatékony megelőző vagy javító intézkedés és csak addig javasolt az alkalmazása ameddig egy hatékony és végleges javító intézkedést be nem vezetünk. Néha az is szükséges lehet, hogy módosítsunk a terméken egy hatékony ellenőrzési lehetőség kialakítása érdekében. A jelenlegi szabályozási rendszer megváltoztatása is eredményezheti a helyzet javulását. A hangsúlynak lehetőleg a megelőzésen kell lenni, ami lehet például SPC alkalmazás, a folyamaton végrehajtott valamilyen fejlesztés, sokkal inkább, mint véletlenszerű ellenőrzések bevezetése.

Ha a csoport a kiértékelés során úgy dönt, hogy nincs szükség egy adott lehetséges meghibásodás esetén javító intézkedésre, akkor a rovatba az „NA” bejegyzést tegyük.

20. A javasolt intézkedések felelőssége

Ebbe az oszlopba írjuk be a megfogalmazott intézkedésekért felelős személy vagy szervezet megnevezését és a tervezett bevezetési határidőt.

21. Bevezetett intézkedés(ek)
A bevezetett intézkedések rövid leírását írjuk ebbe az oszlopba, a bevezetés után.

22. Az intézkedések eredménye
Ha meghatároztunk egy megelőző vagy javító intézkedést, akkor kiértékeljük az új helyzetet a súlyosság, a gyakoriság és a detektálás szempontjából. Kiszámítjuk az új kockázati tényezőt. Ha korábban úgy döntöttünk, hogy nem szükséges javító intézkedés, akkor ezeket az oszlopokat üresen hagyjuk.

Minden újra számolt kockázati tényezőt vizsgáljunk felül, ha szükséges végezzük el újra a meghibásodás elemzését. Mindig a folytonos fejlődésnek kell a figyelem középpontjában állni.

Nyomonkövetés intézkedései
A folyamatért felelős mérnök feladata biztosítani, hogy minden szükséges intézkedést megtegyenek. Az FMEA egy élő dokumentum, ami azt jelenti, hogy minden változást tükröz, akár a termék változásával akár a folyamat módosításaival kapcsolatos, beleértve azokat is, amelyeket a gyártás megkezdése után vezettek be.

A folyamat mérnöknek számos eszköz áll rendelkezésre, hogy megbizonyosodjon az intézkedések bevezetéséről. Ezek és természetesen nem csak ezek, a következők lehetnek:

- Meggyőződni arról, hogy a termék és folyamat követelmények teljesülnek,
- A műszaki dokumentumok, rajzok, folyamat leírások átnézése,
- Meggyőződni arról, hogy a dokumentált változások a gyártási, szerelési folyamatban életbe léptek,
- „Control Plan” és a műveleti utasítások átnézése.

Felhasznált és javasolt irodalom

[1] Bálint Julianna (Szerk.): Minőség – tanuljuk, tanítsuk és valósítsuk meg, TERC Kft. 2001.
[2] Birolini, A.: Qualität und Zuverläßigkeit technischer Systeme, Springer-Verlag, Berlin-Heidelberg- New York, 1991.
[3] Farkas G.: Zuverlässigkeit quasiredundanter Systeme, Dissertation TU Dresden, 1974
[4] Farkas Gy. – Héray T.: Minőség és megbízhatóság, Főiskolai jegyzet, SZIF 2000, Győr
[5] Farkas Gy.: Elektronikus berendezések konstrukciója, Tankönyvkiadó Budapest, 1974
[6] Fischer, K.: Zuverläßigkeits- und Instandhaltungstheorie, Transpress Verlag, Berlin, 1984.
[7] Gaál Z. – Kovács Z.: Megbízhatóság, karbantartás, Veszprémi Egyetem Kiadói Iroda, Veszprém, 1994.
[8] Gnyegyenko, B.V. – Beljajev, J.K. - Szolovjev, A.D.: A megbízhatóságelmélet matematikai módszerei, Műszaki Könyvkiadó, Budapest, 1970.
[9] Győrfi L., Pali I.: Tömegkiszolgálás informatikai rendszerekben, Műegyetemi Kiadó Budapest, 1996
[10] Héray T.: Biztonság és megbízhatóság a műszaki gyakorlatban, SZIF Győr, 1985
[11] Howard R.: Dynamic programming and Markov processes, M.I.T. Press 1962
[12] Kamiske, G.F. – Brauer, J.P.: Qualitäts-management von A bis Z., Hanser Verlag, München–Wien, 2003.
[13] Kleinrock L.: Sorbanállás kiszolgálás, Műszaki Könyvkiadó Budapest, 1979
[14] Konakovsky, R.: Sichere Prozeßdatenverarbeitung mit Mikrorechnern, Oldenbourg Verlag, München-Wien, 1988.
[15] Kun I. – Szász G. – Zsigmond Gy.: Minőség és megbízhatóság I-II., LSI Informatikai Oktatóközpont, Budapest 2004.
[16] Polonko – Malinova: Szbornyik zadacs po tyeorii nagyozsnosztyi, Sz. Radio 1972
[17] Prékopa: Valószínűség elmélet, Műszaki Könykiadó Budapest, 1972 .
[18] Reinschke: Zuverlässigkeit von Systemen, VEB Technik Berlin, 1973.

[19] Stange, K. – Henning, H.J.: Formeln und Tabellen der mathematischen Statistik, Springer-Verlag, Berlin-Heidelberg- New York, 1966.
[20] Usakov: Metodű resenyia zadacs optimalnovo rezerviroványia, Sz. Radio 1969.
[21] Vincze István: Matematikai statisztika – ipari alkalmazásokkal, Műszaki Könyvkiadó, Budapest 1968.