Biztonságkritikus rendszerek

Dr. Abonyi, János

Dr. Fülep, Tímea

Szerzők: Abonyi János (Fejezet 1-9) és Fülep Tímea (Fejezet 10-12)

A tananyag a **TÁMOP-4.1.2.A/1-11/1-2011-0042** azonosító számú
„ ***Mechatronikai mérnök MSc tananyagfejlesztés*** ” projekt keretében készült. A tananyagfejlesztés az Európai Unió támogatásával és az Európai Szociális Alap társfinanszírozásával valósult meg.

Kézirat lezárva: 2014 február

Lektorálta: Dr. Feil Balázs

A kiadásért felel a(z): Pannon Egyetem

Felelős szerkesztő: Pannon Egyetem

2014

Biztonságkritikus rendszerek

Abonyi János (1-9 fejezetek)

Fülep Tímea (10-12 fejezetek)

Tartalom

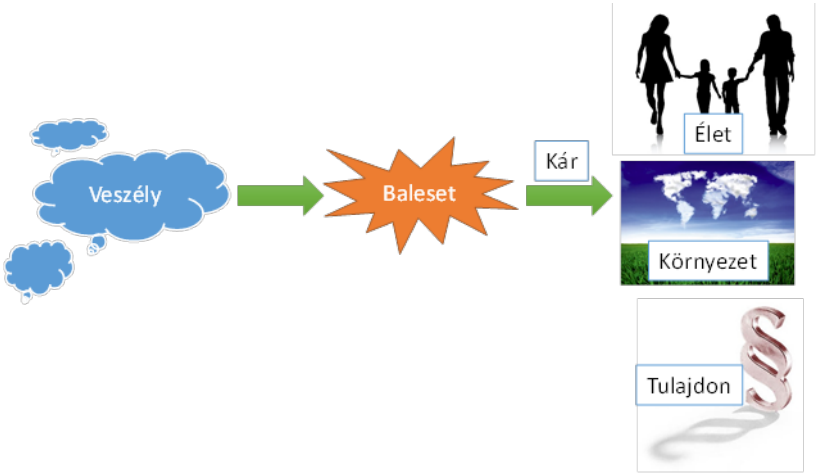
Ábrajegyzék

1 Kockázatelemzés alapjai

„Ami elromolhat, az el is romlik.” Ezt az örökérvényű felismerést Edward Murphy mérnöknek köszönhetjük, és onnan eredeztetjük, hogy 1948–49 között a Wright-Patterson amerikai légitámaszponton a gyorsulás emberi szervezetre kifejtett hatását vizsgáló kísérletsorozatot a rosszul felszerelt mérőműszerek miatt elölről kellett kezdeni. A nem kívánt eseményekhez - mint például egy műszaki rendszer meghibásodásához - társítható kockázatok értékeléséhez kapcsolódó alapfogalmak bemutatása könyvünk első fejezetének célja. E fogalom-meghatározások során gyakorta hivatkozni fogunk a kockázatmenedzsmenttel és biztonságkritikus rendszerekkel kapcsolatos szabványokra.

1.1 Alapvető koncepciók: kockázat és veszélyeztetés kapcsolódó fogalmai

Egy nem kívánt esemény, egy meghibásodás következményei egy kísérlet megismétlésével járó kellemetlenségeknél súlyosabbak is lehetnek. Veszélybe kerülhet emberi élet, a természeti környezet, vagy anyagi kár is bekövetkezhet (1.1. ábra).



1.1. ábra. Életben, környezetben és tulajdonban kárt okozó baleset, mint veszélyhelyzet.

A kár/sérülés (angolul harm) fogalom a baleset bekövetkeztének életre, egészségre, környezetre és anyagi javakra vonatkozó elkerülendő eredményét jelöli. A biztonság e szempontból nem más, mint a kár bekövetkeztének elkerülése, azaz ahogy a MIL-ASTD882B:1984-es szabvány definiálja: a biztonság mentesség olyan feltételektől, körülményektől melyek bekövetkezése halált, sérülést, foglalkozási ártalmat, készülékben, tulajdonban károsodást, illetve üzleti veszteséget okoz.

A kár/sérülés (angolul harm) fogalom a baleset bekövetkeztének életre, egészségre, környezetre és anyagi javakra vonatkozó elkerülendő eredményét jelöli. A biztonság e szempontból nem más, mint a kár bekövetkeztének elkerülése, azaz ahogy a MIL-ASTD882B:1984-es szabvány definiálja: a biztonság mentesség olyan feltételektől, körülményektől melyek bekövetkezése halált, sérülést, foglalkozási ártalmat, készülékben, tulajdonban károsodást, illetve üzleti veszteséget okoz.

Mindezt tömören összefoglalják IEC 50(191) szabvány fogalom meghatározásai:
Sérülés [harm]*: az egészség, az anyagi javak vagy a környezet sérülése, illetőleg károsodása.
Veszély [hazard]*: potenciális sérülés forrása, vagy potenciális sérülést jelentő helyzet, azaz a veszély potenciális kárforrás (IEC 61508/61551)
Veszélyes esemény [hazardous event]: sérülés okozására képes esemény.

Veszélyeztetés ennek megfelelően nem más, mint egy nem kívánt esemény bekövetkezésének lehetősége, azaz olyan helyzet, amelyben személyek vagy a természeti, gazdasági és műszaki környezet potenciálisan veszélyben van.

Fontos megjegyezni, hogy műszaki rendszerek esetében tipikus veszélyhelyzet az, amikor egy eszköz, anyag, illetve készülék magasabb energiaszinten van, mint a környezete és eltérés van a tervezett üzemállapottól, paramétertől.

A hatások szerint többféle veszélyt különböztethetünk meg.

1.1. táblázat. Veszélykategóriák

Veszélykategóriák	Következmények (Baleset)	Hatások (Kár)
Természeti	Árvíz, földrengés, környezeti szennyezés	Társadalmi, környezeti és egyéni kár, haláleset
Technológiai	Ipari és közlekedési balesetek	Társadalmi, könnyezeti és egyéni kár, haláleset
Társadalmi	Háború, terrorcselekmény, szabotázs	Társadalmi, környezeti és egyéni kár, haláleset

Nagyon fontos, hogy az különbséget tegyünk a veszély (Hazárd) és a kockázat (Risk) között. A veszélyeztetés (hazárd) a baleset bekövetkezésének lehetőségét reprezentálja, míg a kockázat magába foglalja azokat a forgatókönyveket, melyek a nem kívánt esemény bekövetkezéséhez társíthatók, meghatározva azok bekövetkezésének valószínűségét is.

Minden veszélyeztetéshez hozzárendelhető tehát egy bizonyos kockázat, amely függ az esemény bekövetkezésének valószínűségétől és az esemény következményeinek súlyosságától.

A kockázat [risk] tehát valamely adott veszélyes esemény előfordulása gyakoriságának vagy valószínűségének (F), valamint a következmény súlyosságának (C) a kombinációja:

$$R = C \times F \tag{1.1}$$

Ahogy az egyenlet sugallja, kis kockázata van rendkívül ritkán bekövetkező kis kárértékű veszélyhelyzeteknek, illetve a kockázat nő a bekövetkezés gyakoriságának (bekövetkezési valószínűségének) és a következmény súlyosságának növekedésével.

Egy komplex, egymástól független elemekből álló rendszer esetében a **teljes kockázat** az egyes, egymástól független veszélyeztetésekhez kapcsolódó kockázatok összegeként határozható meg:

$$R = \sum_{i=1}^{n} C_i \times F_i \tag{1.2}$$

A jegyzet elsősorban a műszaki kockázatok kezelésére és elemzésére fókuszál. A **műszaki kockázat** (Technical Risk) annak mértéke, hogy az érdekelt felek (felhasználók, tulajdonosok, társadalom) elvárásai és a műszaki követelmények mennyire teljesülnek egy technológia rendszer termékéhez illetve működtetéséhez kapcsolódóan.
E meghatározáshoz szorosan kapcsolódik a **rendszer** fogalma [system], miszerint a rendszer egységes egész, amely tetszőleges bonyolultságú ember, eljárásrend, anyag, eszköz, berendezés, létesítmény és szoftver alrendszerekből állhat. A rendszert, mint elemekből álló egységes egészet együttesen

alkalmazzák az előírt működési vagy kiszolgáló környezetben egy adott feladat, illetve cél teljesítésének érdekében. Ennek megfelelően a kockázatot magára termékre, illetve a termelési folyamatra vonatkozóan is elemezhetjük.

A kockázatmenedzsment legfontosabb célja a biztonság (safety) megfelelő szintű biztosítása. Ennek alapja a kockázatok azonosítása és minősítése. Előfordulhat, hogy egy veszélyhelyzet kockázatát nem tudjuk teljes mértékben minősíteni. A **nem azonosított kockázat** (Unidentified Risk) az a kockázat, amit nem határoztak meg, míg az **azonosított kockázat** (Identified Risk) az a kockázat, amely különböző elemzési technikákkal meghatározható.

Elfogadható (tolerálható) kockázat (Acceptable vagy tolerable risk) az azonosított kockázat azon része, amely további csökkentés nélkül is megengedett. Az elfogadható kockázat tehát az a kockázat, amely az érintettek (tervező, megrendelő, felhasználó, társadalom) számára elfogadható. A halálos kimenetelű közlekedési balesetek száma hazánkban 2012-ben 541 volt (a közel 10 milliós népességből). Az a tény, hogy naponta részt veszünk a közlekedésben igazolja, hogy elfogadjuk ezt a kockázatot, azaz a társadalom számára ez a szám elfogadható kockázatot jelent. Ennek ellenére természetesen folyamatosan szem előtt tartott célkitűzés a közúti balesetek számának csökkentése. E példa jól mutatja, nem egyszerű feladat, hogy miként definiáljuk, hogy hol van az elfogadható kockázat határa. Mindezek ellenére, az elfogadható kockázat meghatározása kulcsfeladat, ugyanis ez ad a kockázatcsökkentési tevékenység számára iránymutatást.

A **nem elfogadható kockázat** (Unacceptable Risk) az azonosított kockázat azon része, amit vagy megszüntetni, vagy csökkenteni kell.

A **fennmaradó kockázat** (Residual Risk) az azonosított kockázat azon része, ami a teljes kockázatkezelési folyamat után a kockázatcsökkentési tevékenység eredménye után megmarad és mértéke a sikeres kockázatmenedzsment esetén alacsonyabb mint az elfogadható kockázat.

A **biztonság** (safety) tehát nem más, mint „Mentesség olyan feltételektől melyek bekövetkezése halált, sérülést, foglalkozási ártalmat, készülékben, tulajdonban károsodást és veszteséget, illetve üzleti veszteséget okozhat (MIL-ASTD882B). Biztonságról tehát akkor beszélhetünk, ha a kockázatértékelés során megállapítjuk, hogy nincs nem elfogadható kockázat, illetve olyan sikeres kockázatcsökkentési tevékenységet végeztünk, mely hatására a kockázat az elfogadható kockázati szintre csökkent (Mindez az ISO/IEC guide 50 szerint a biztonság definíciója).

Más értelmezésben a **biztonság** (safety, S)– ellenálló képesség, azaz a veszélyeztetettségtől mentes állapot valószínűsége, azaz

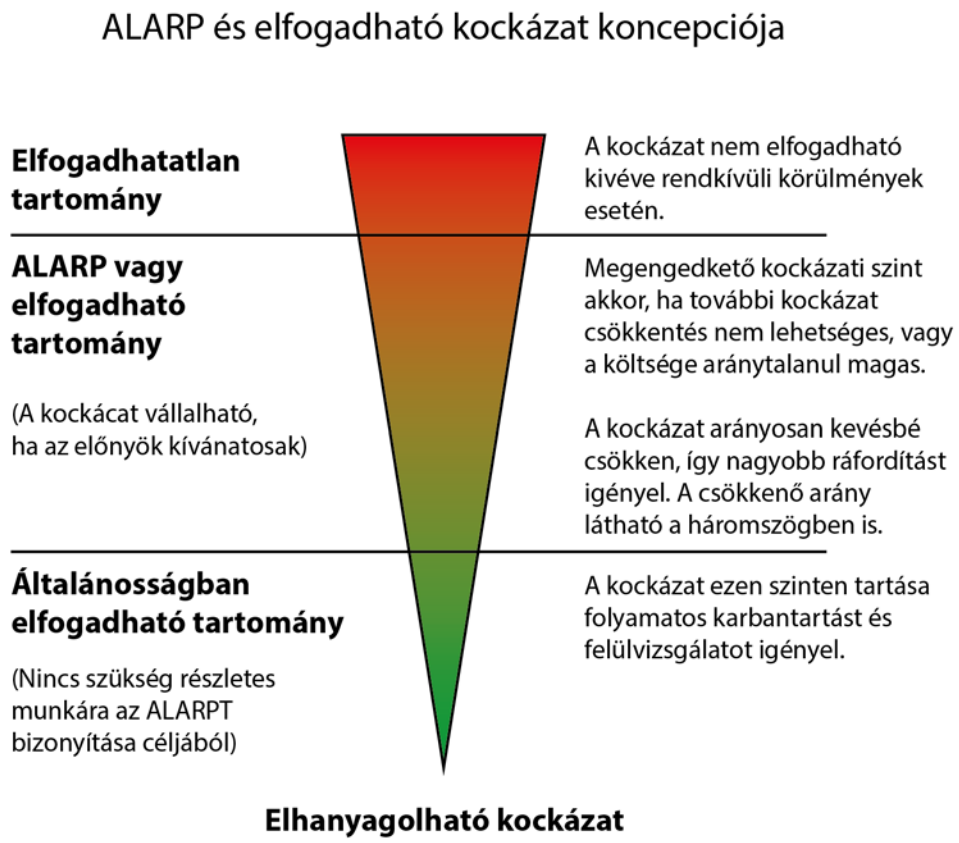
$$S = 1/R \tag{1.3}$$

A **funkcionális biztonság**ot az IEC 61508 szabvány az E/EP rendszerek hibából eredő meghibásodásokra visszavezethető nem megengedhető kockázattól való menteségként definiálja.

1.2 A szükséges kockázatcsökkentés meghatározása – ALARP alapelv

A műszaki rendszer tervezőjének és üzemeltetőjének általános kötelessége a kockázat "lehető legkisebb ésszerűen megvalósítható" (angol rövidítéssel: ALARP) szintre való csökkentése. Ugyanakkor tekintettel arra, hogy a kockázat nem szüntethető meg teljesen, szükségszerűen létezik arányosság a kockázat és annak csökkentésére irányuló intézkedések között. E kérdésből adódik a

kockázatcsökkentés szükséges mértékének meghatározása, mely során az alábbi ábrán ismertetett ALARP alapelv is iránymutató.

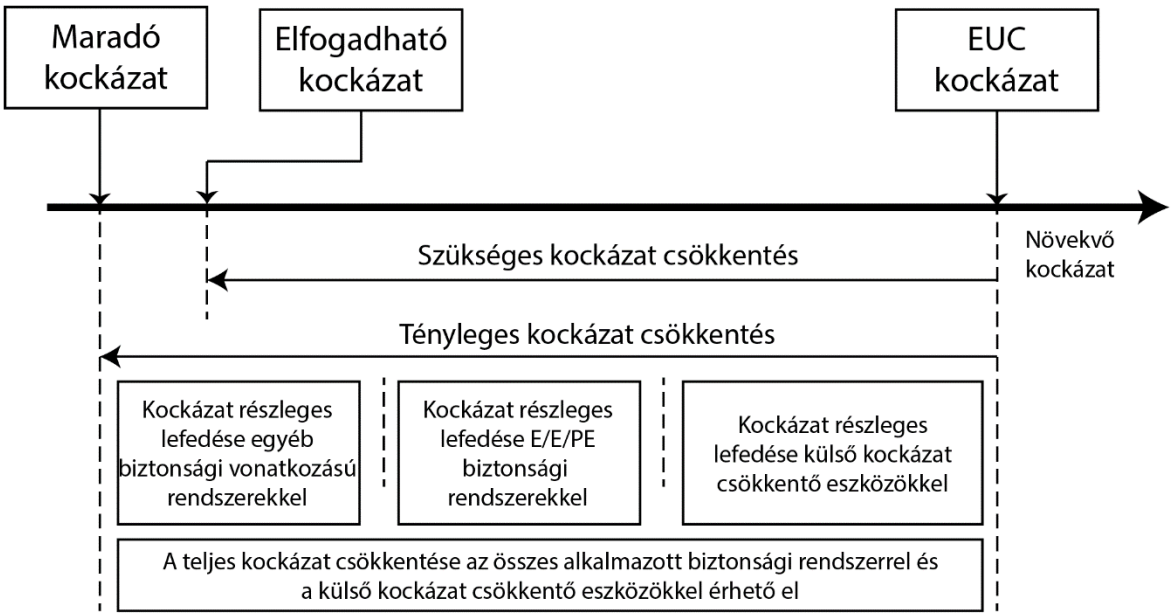


1.2. ábra. As Low as Reasonable Possible (ALARP) alapelv szemléltetése

A fenti ábra jól mutatja, hogy a biztonságkritikus műszaki rendszert tervező mérnök három eshetőséggel találkozhat:

- A feltárt kockázat kizárólag csak extrém körülmények között fogadható el.
- Vannak olyan esetek, amikor a kockázat elfogadható mértékű. Ezekben az esetekben a mérnök elengedhetetlen feladata, hogy részletesen elemezze miként érvényesíthető az ALARP alapelv, és kizárólag csak akkor ne végezzen el további kockázatcsökkentési tevékenységet, ha az nem kivitelezhető vagy a kivitelezés költsége nem áll arányban a várható előnyökkel. A kockázat akkor is tolerálható, ha a veszélyhelyzetet jelentő műszaki rendszer általánosan előnyös a társadalomra és az emberekre, és ezen előnyök mértéke messze meghaladja a kockázat mértékét (pl. atomenergia).
- Azokban az esetekben, amikor a kockázat általánosságban is elfogadható, nincs szükség a kockázat további csökkenthetőségének elemzésére.

A szükséges kockázatcsökkentést mindig egy-egy meghatározott veszélyes esemény szempontjából kell értékelni. az E/E/PES (Elektromos / Elektronikus / Programozható elektronikus) rendszerek esetében az IEC 61508 szabvány írja elő a kockázat csökkentésének módszertanát (1.3. ábra).



1.3. ábra. A kockázat csökkentésének folyamata

Tekintsünk egy kockázatos, EUC (szabályozott rendszerhez kapcsolódó) rendszert melynek kockázatát és a rendszerre vonatkozó elfogadható kockázatot meghatároztuk. Amennyiben az azonosított kockázat nagyobb, mint az elfogadható, a rendszer módosításával megfelelő kockázatcsökkentési lépéseket kell végrehajtani. E kockázatcsökkentés általában a rendszer olyan új funkciókkal történő bővítését tarkarja mely új funkciók alkalmasak a kockázatos eseményhez kapcsolódó hibák elkerülésére, eltávolítására vagy detektálására vagyis a kockázat csökkentésére. A rendszer módosítását követően a fennmaradó kockázatnak (residual risk) az elfogadható kockázat alá kell csökkennie.

E kockázatcsökkentési tevékenység szellemében az IEC 61508 szabvány a következő fontos állításokat fogalmazza meg:

- kockázatmentes állapot soha nem érhető el
- a biztonságot már a tervezési folyamat elején figyelembe kell venni
- a nem elfogadható kockázatot feltétlen csökkenteni, menedzselni kell

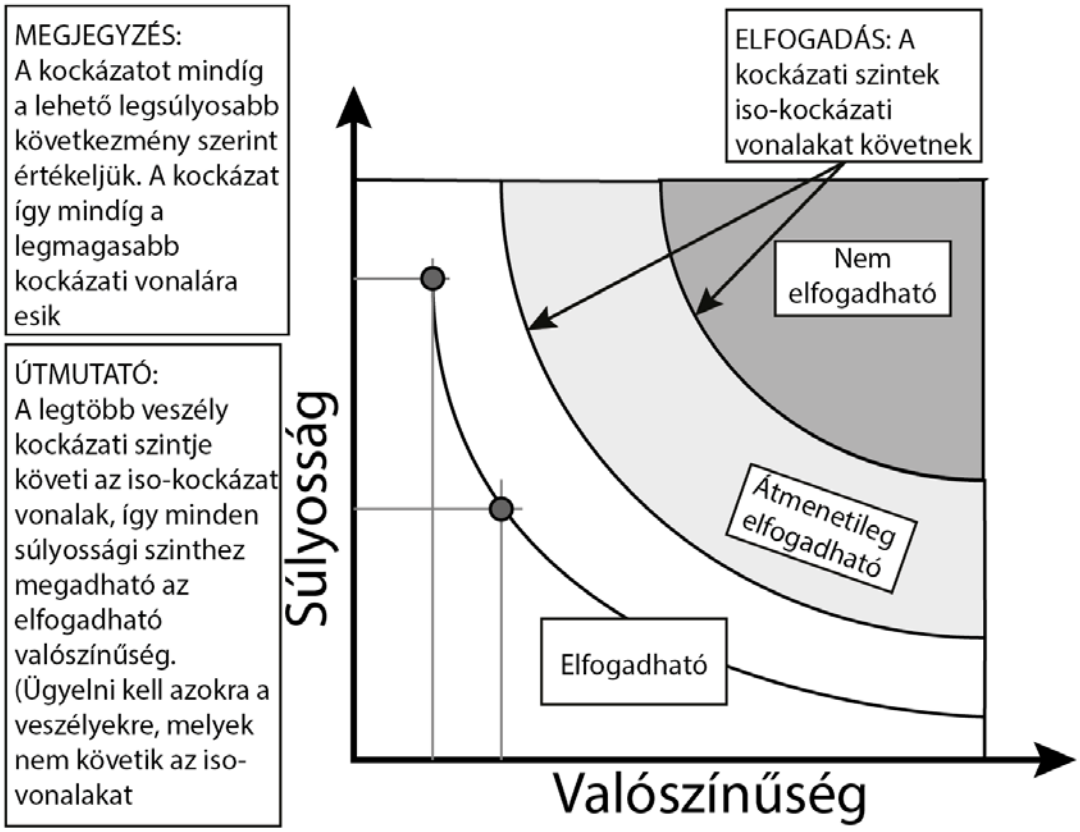
A szükséges kockázatcsökkentést mennyiségi és/vagy minőségi módszerek alkalmazásával kell meghatározni. A kockázatértékelésre alkalmas technikák közül ebben a bevezető fejezetben a kockázati mátrix alkalmazási lehetőségeit mutatjuk be.

1.3 Kockázati mátrix

A kockázatértékelési mátrix egy, a kockázat alapvető definícióján alapuló kvalitatív kockázatértékelési eszköz. Ez az alfejezet a NASA *System Engineering "Toolbox" for Design-Oriented Engineers* anyaga alapján ismerteti ezen eszköz alkalmazásának részleteit.

Tekintettel arra, hogy a kockázat a nem kívánt esemény következményének súlyossága és a bekövetkezés valószínűségének szorzata, a következmény súlyossága és a bekövetkezés gyakorisága

által definiált koordináta rendszerben az azonos kockázati szinteket jelentő pontokat összekötő, úgynevezett iso-kockázat görbék képezik e technika alapját (1.4. ábra).



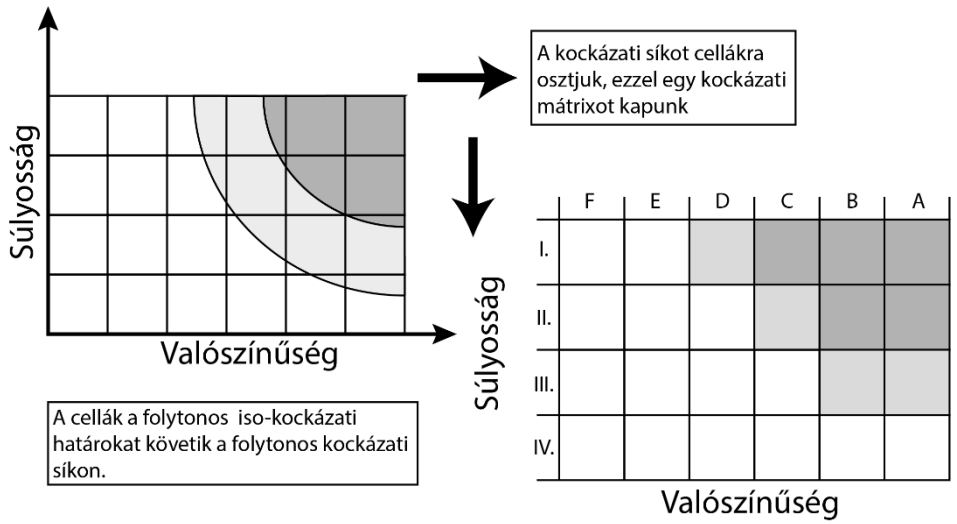
1.4. ábra. Kockázati térkép és az iso-kockázati szintek

Ezek az azonos kockázati szinteteket reprezentáló görbék rendkívül hasznosak, ugyanis útmutatóul szolgálnak a kockázat értékelésében, az elfogadható kockázat meghatározásában.

A technikát előzetes kockázatelemzésre alkalmazzák, az adott nem kívánt eseményhez társítható veszélyhelyzetet a következmény súlyosságával és a bekövetkezés valószínűségével jellemezve. Az alkalmazás folyamata a következő:

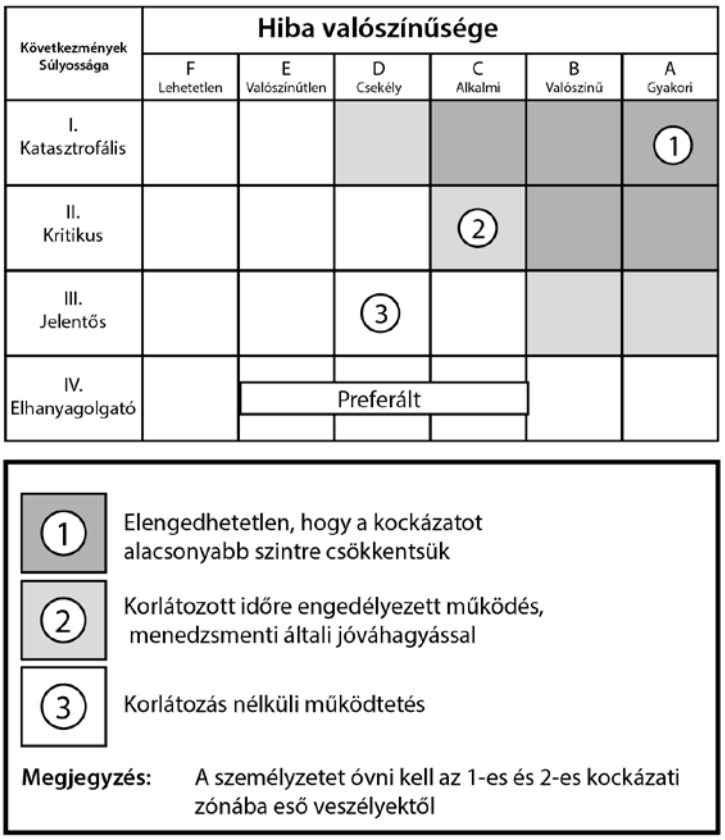
1. Kategorizáld a nem kívánt események bekövetkezési valószínűségét. A technika szubjektív, így ennek megfelelően a kategóriák: gyakori, valószínű, alkalmi, a távoli jövőben talán várható, valószínűtlen és lehetetlen (a MIL–STD–882C szabvány szerint a következő angol kifejezéseket alkalmazhatók: frequent, probable, occasional, remote, improbable, and impossible).
2. Kategorizáld a következmény súlyosságának mértékét szubjektív következményi skálát alkotva, mint például katasztrofális, kritikus, marginális, elhanyagolható
3. Készíts egy mátrixot a két változó felhasználásával. Közelíts az iso-kockázati görbéket a mátrix celláival. A mátrix cellái rögzítik a kockázat elfogadható értékét. Fontos megjegyezni, hogy az elfogadható kockázat értékét nem az adott kockázatot elemző, hanem a kockázatmenedzsmentet végzők határozzák meg.

4. Kalibráld a kockázati mátrixot egy – egy cella kiválasztásával és a gyakorlatban előforduló veszélyhelyzet hozzárendelésével. E veszélyhelyzet ismerős kell, hogy legyen az elemző számára, illetve meghatározható kell legyen annak elfogadhatósága. Ez és más hasonló jellegű kalibrációs pontok benchmarkként szolgálnak a további, adott esetekhez hasonló kockázatok értékelésében.

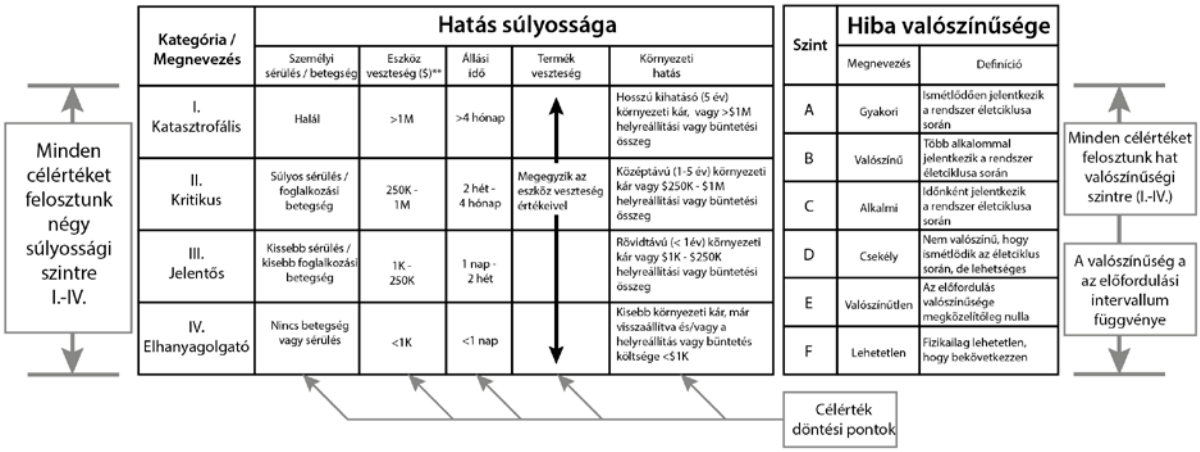


1.5. ábra. Az iso-kockázati görbék közelítése a kockázati mátrix celláival.

Példaként tekintsünk egy kockázati mátrixot a MIL–STD–882C szabvány alapján, melynek értékelési rendszerét az alábbi ábra mutatja.



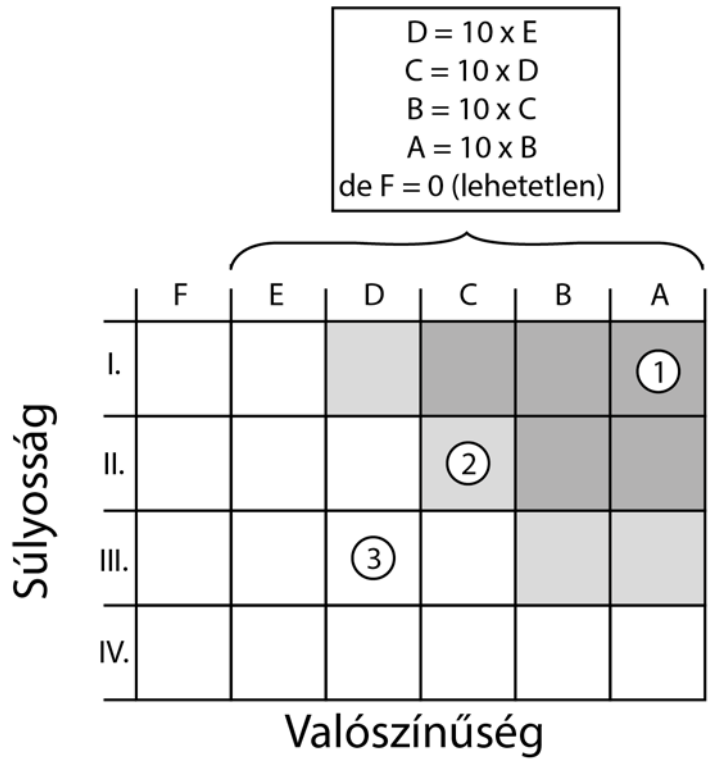
1.6. ábra. Példa kockázati mátrixra a a MIL–STD–882C szabvány alapján.



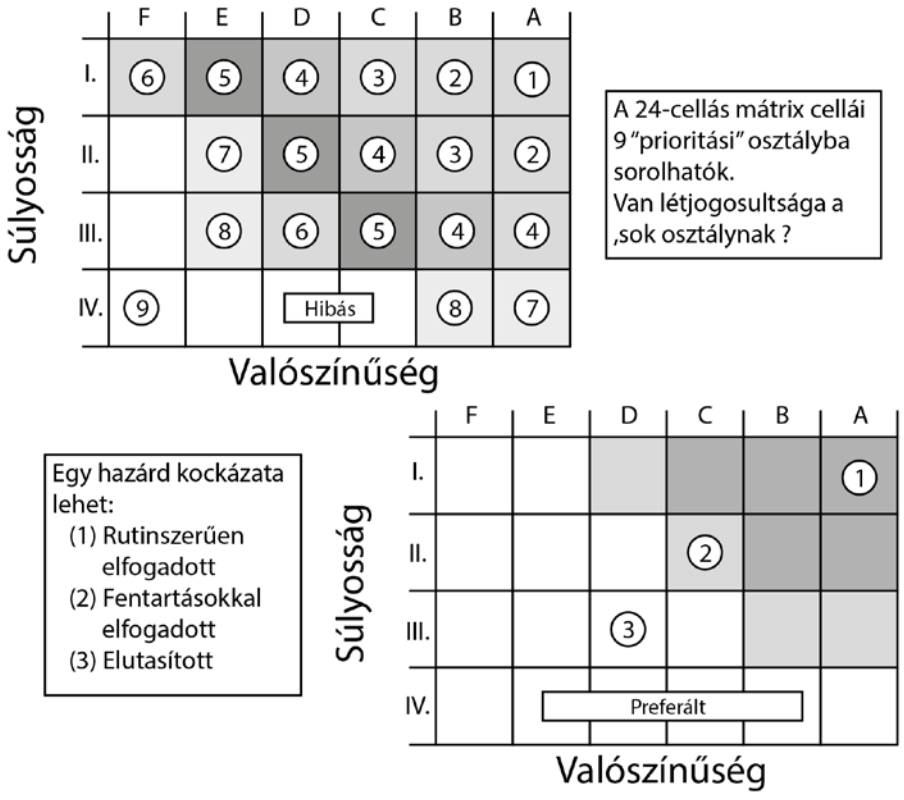
1.7. ábra. Az előző ábrán definiált kockázati mátrix értékelési rendszere.

A mátrix készítéskor a következő szempontokat érdemes szem előtt tartani:

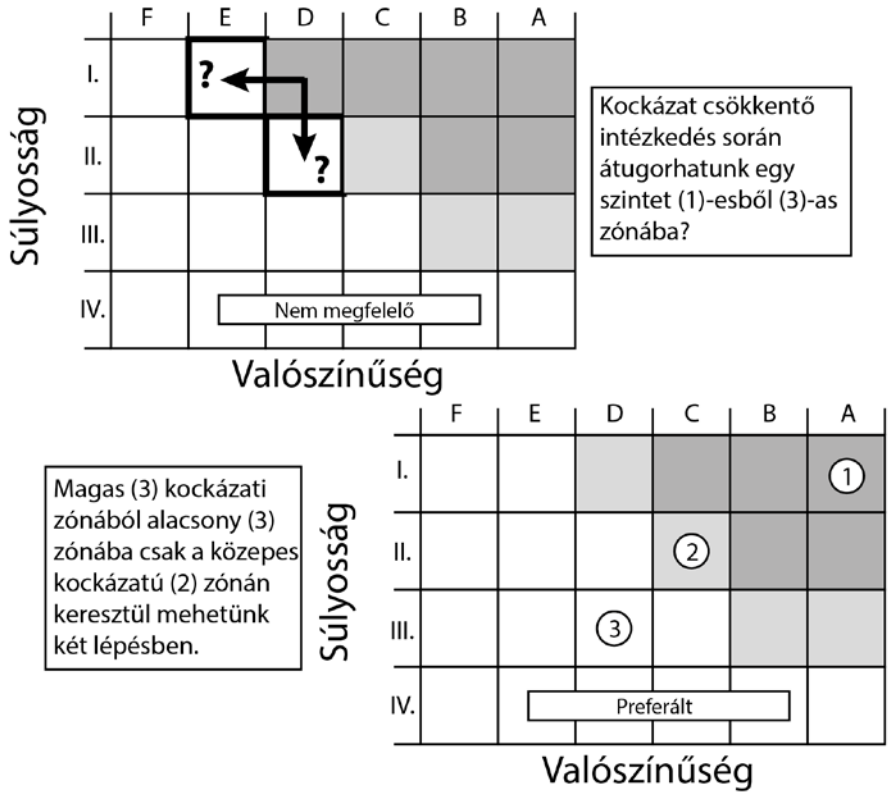
- Ne alkoss túl sok kategóriát, illetve túl sok cellát a márixban. Az értékelési technika szubjektív, így túl részletes skála kevésbé konzisztensé teheti az értékelést.
- Kockázati szintből is kevés zónát alkoss, pl., (1) elfogadhatatlan, (2) megkötésekkel, kompromisszumként átmenetileg elfogadható, (3) általában elfogadható.
- A kockázati zónáknak folytonosnak kell lenniük, azaz egy lépésből csak egy kockázati szinttel eltérő zónába lehessen eljutni (lásd alábbi ábra).



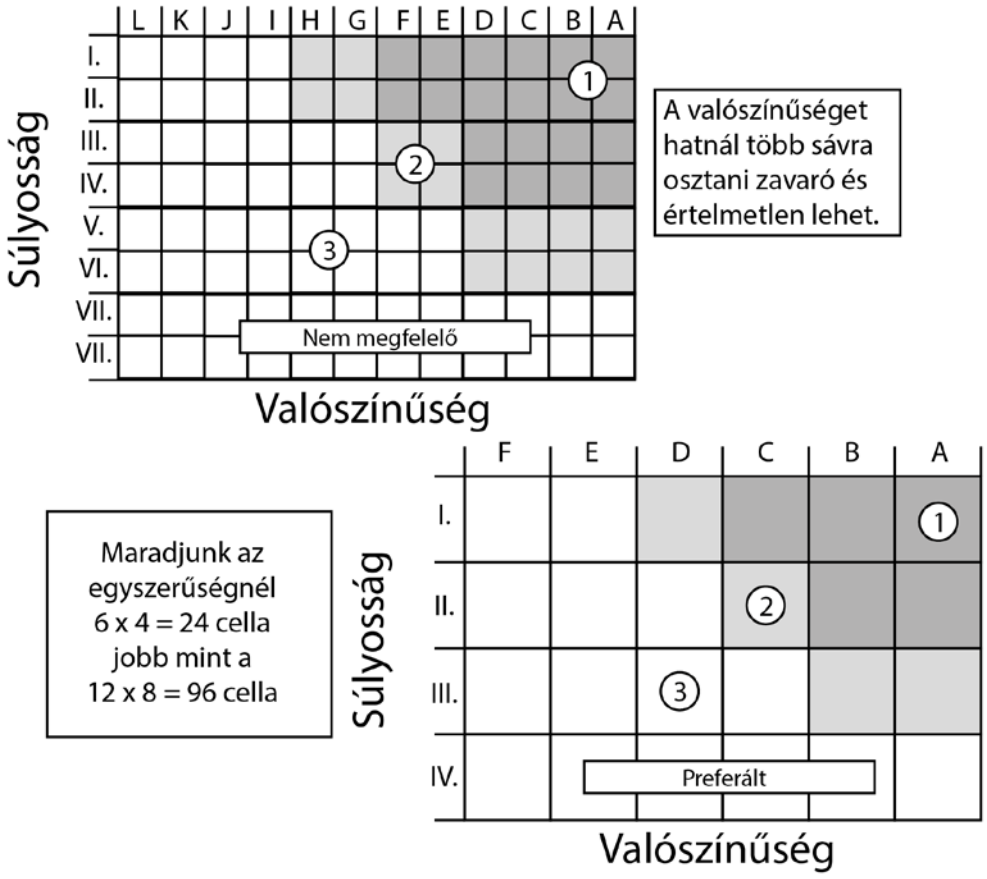
1.8. ábra. A kockázati mátrix hasznos felbontása



1.9. ábra. A kockázati mátrix definiálásának alapelvei I.



1.10. ábra. A kockázati mátrix definiálásának alapelvei II.



1.11. ábra. Példa kockázati mátrix redukciójára (azaz ne használjunk feleslegesen részletes felbontást)

A technika sajátosságait összefoglalva tekintsük át annak előnyeit és hátrányait.

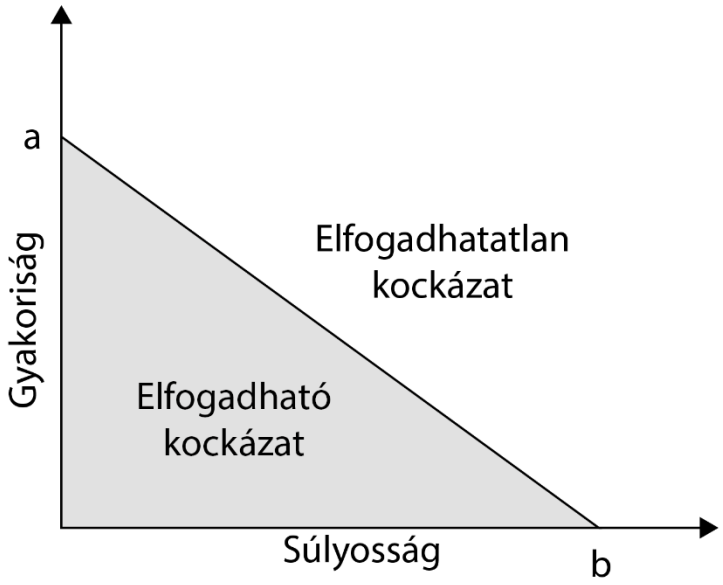
Előnyök:

- A módszeres mérnöki munkát megfelelően támogatja.
- Adott kockázathoz tartozó következmény súlyosságának és a bekövetkezés gyakoriságának áttekinthető reprezentációját biztosítja.
- A nem elfogadható kockázatok megfelelő azonosítására alkalmas. A kockázat csökkentésének szándékolt módja könnyen vizualizálható. (Érdemes megjegyezni, hogy a passzív biztonsági elemek következmény súlyosságát csökkentve csökkentik a kockázatot, míg az aktív biztonsági megoldások elsődlegesen a bekövetkezés valószívűségét csökkentik).

Hátrányok:

- A technika csak előre definiált vészhelyzetek értékelésére alkalmas, nem támogatja új kockázati helyzetek feltárását.
- A módszer szubjektív, leginkább összehasonlító jellegű elemzéseket tesz lehetővé.

A módszer alkalmazásával kapcsolatban fontos megjegyezni, hogy a kockázati mátrix, illetve a hasonló jelegű elemzések alapján az elvárt biztonságból és a következmények súlyosságából meghatározható a rendszer-meghibásodások kívánt/elfogadható szintje (1.12. ábra)



1.12. ábra. A nem kívánt események gyakorisága meghatározható az elfogadható kockázat értékéből.

E célból közvetlenül a kockázati mátrix kategóriái vagy az iso-kockázati görbe egyenlete, vagy az alábbi, az elfogadható kockázat mértékét közelítő, illetve definiáló egyenlet alkalmazható:

$$\frac{gyakoriság}{a} + \frac{következmény}{b} < 1 \qquad (1.4)$$

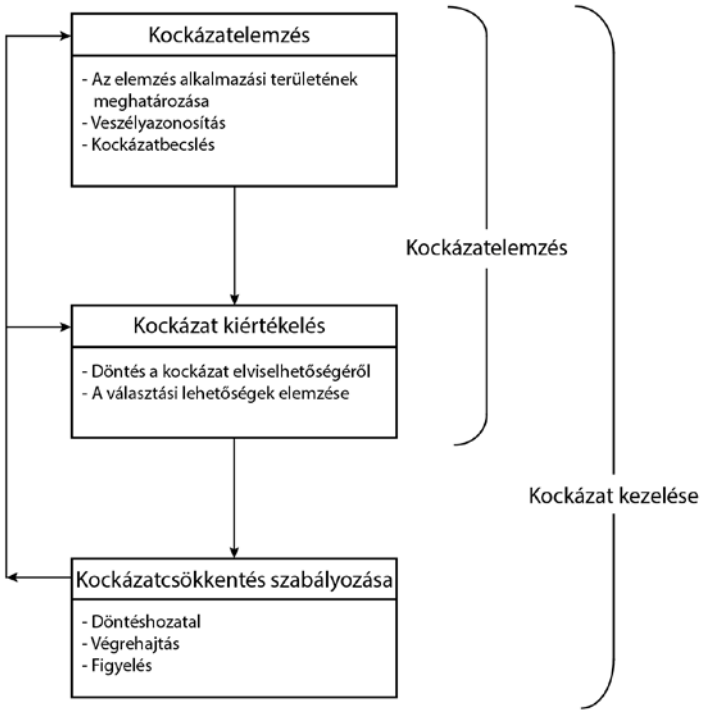
ahol az a csaknem elhanyagolható következményű események maximálisan tolerálható gyakorisága, és b az azon esemény következményének súlyossága melynek bekövetkezési valószínűsége csaknem elhanyagolható.

2 Kockázatelemzés és kockázatmenedzsment

Az előző fejezetben a kockázathoz kapcsolódó alapfogalmakat tekintettük át. E fejezet célja a kockázatmenedzsment folyamatának, módszertanának a bemutatása, leginkább az IEC 50(191) és az IEC 60508 szabványok fogalom-meghatározásait alkalmazva.

2.1 Kapcsolódó fogalmak

A **kockázat kezelés, kockázat menedzsment** [risk management] a kockázatelemzési, kockázatkiértékelési és kockázatszabályozási feladatokkal kapcsolatos irányítási elvek, eljárásrendek és gyakorlat módszeres alkalmazását jelenti. Ahogy az alábbi ábra mutatja, a kockázatok kezelése kockázatértékelés és kockázat csökkentés/szabályozási lépésekből áll.



2.1. ábra. A kockázatmenedzsment folyamata.

A **kockázatelemzés** [risk analysis] a rendelkezésre álló információk módszeres felhasználása a veszélyek azonosítása érdekében. A kockázatelemzés az elemzés alkalmazási területének meghatározását, a kapcsolódó veszélyek azonosítását és a kockázat becslését foglalja össze.

A **kockázatértékelés** [risk assessment] kockázatelemzési és kockázatkiértékelési részfolyamatokra osztható.

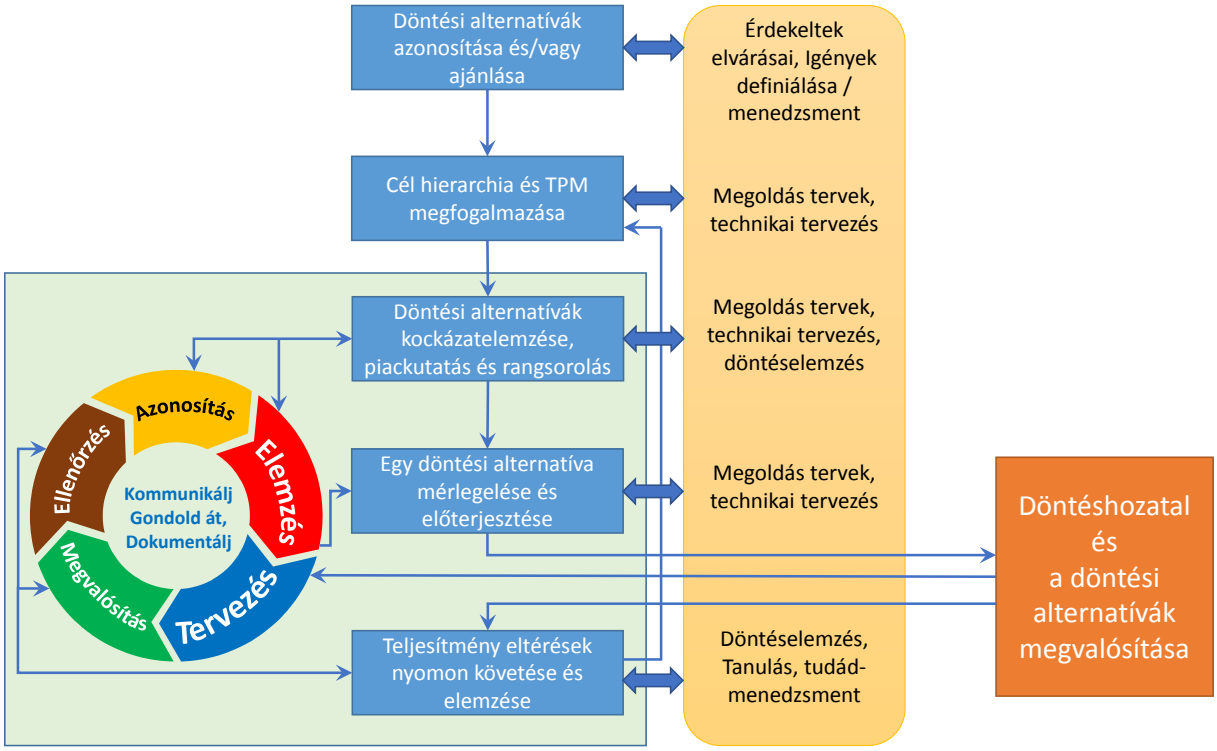
Veszélyazonosítás [hazard identification] alatt a veszély meglétének felismerésére és jellemzőinek meghatározására vonatkozó eljárást értjük.

A **kockázatbecslés** [risk estimation] az elemzett kockázatok mértékének meghatározására használatos eljárás. A kockázatbecslés a következő lépésekből áll: gyakoriságelemzés,

következményelemzés és ezek integrálása. A kockázatértékelés második lépése a kockázatkiértékelés (kockázat-megítélés) [risk evaluation]: olyan folyamat, amelynek során a kockázatelemzés alapján kiértékelik a kockázat elfogadhatóságát.

A **kockázatszabályozás** [risk control]: a kockázatok kezelésével és/vagy a kockázatok csökkentésével összefüggő döntéshozatali folyamatot jelenti.

A **folyamatos kockázatmenedzsment** [Continuous Risk Management (CRM)] széles körben alkalmazott technika, amely például kockázati elemeket tartalmazó projektek menedzsmentjére is alkalmas. A CRM iteratív és adaptív folyamat, mely minden tevékenysége az előzőre épül, felhasználva a korábbi lépések során feltárt információkat, folyamatosan csökkentve a kockázatot. A módszertan a következő, alábbi ábrán feltüntetett lépésekből áll:

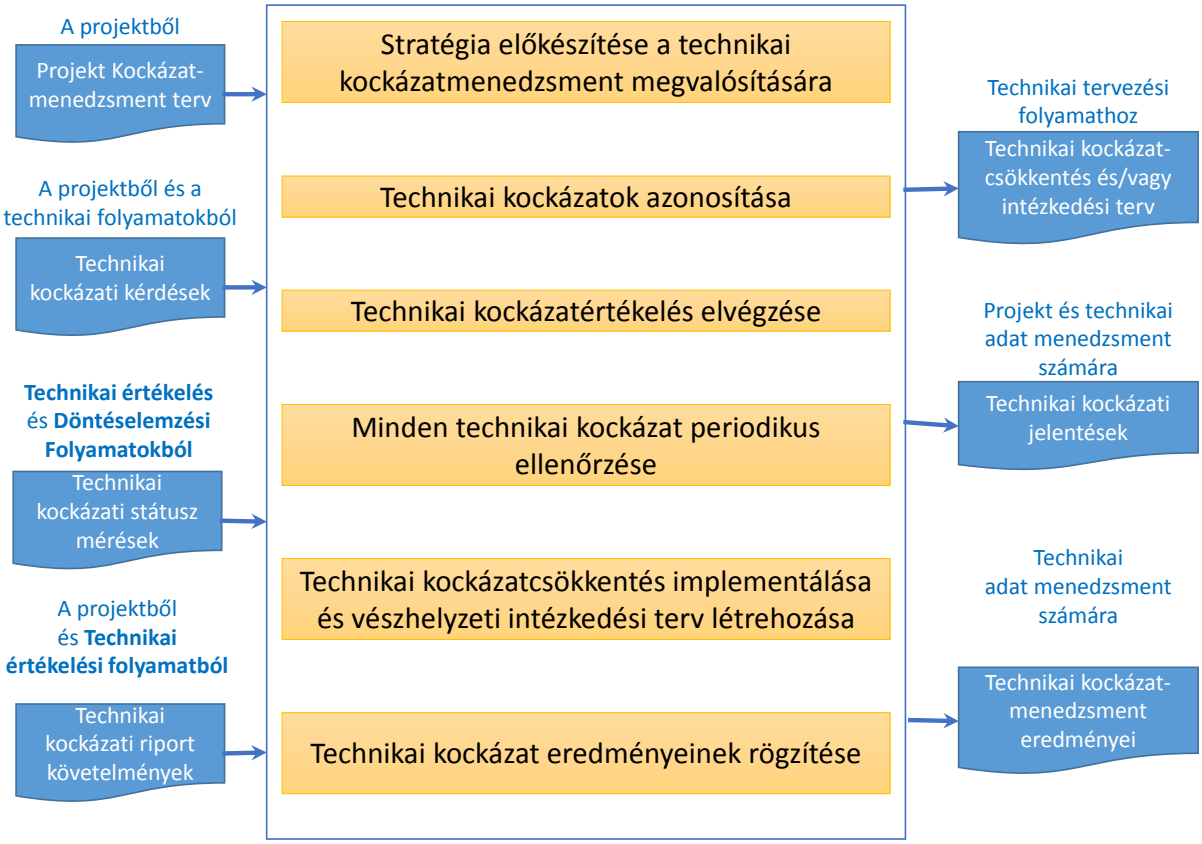


2.2. ábra. A folyamatos kockázatmenedzsment lépései.

- **Kockázat azonosítása** (Identify): E lépés során azokat a nem kívánt eseménysorokat tárjuk fel melyek következményei kockázatot jelenthetnek.
- **Kockázat elemzése** (Analyze) tevékenység a nem kívánt események bekövetkezési valószínűségét és következményének súlyosságát határozza meg, illetve feltárja, hogy mik azok a potenciális eszközök melyek a kívánt időtartam alatt alkalmasak a kockázat kezelésére.
- **Kockázatcsökkentés tervezése** (Plan): A szükséges kockázatcsökkentési lépések meghatározása.
- **Figyelemmel kísérés** (Track): Az előző lépésben meghatározott követelmények megvalósulásának folyamatos figyelemmel kísérése, azaz a teljesítménymutatók és célértékeik folyamatos összevetése.
- **Control** (Ellenőrzés, beavatkozás): Amennyiben szükséges, a megfelelő korrekciók elvégzése, a beavatkozások hatásának visszamérése.

- **Kommunikáció, dokumentálás** (Communicate, Deliberate, and Document) tevékenység minden lépés zárásaként elvégezendő. A kockázatmenedzsmentet érintő dokumentumokat az alábbi ábra tekinti át.

Az alábbi ábra a műszaki kockázatmenedzsment folyamatát mutatja a bemenő és kimenő információk szempontjából.



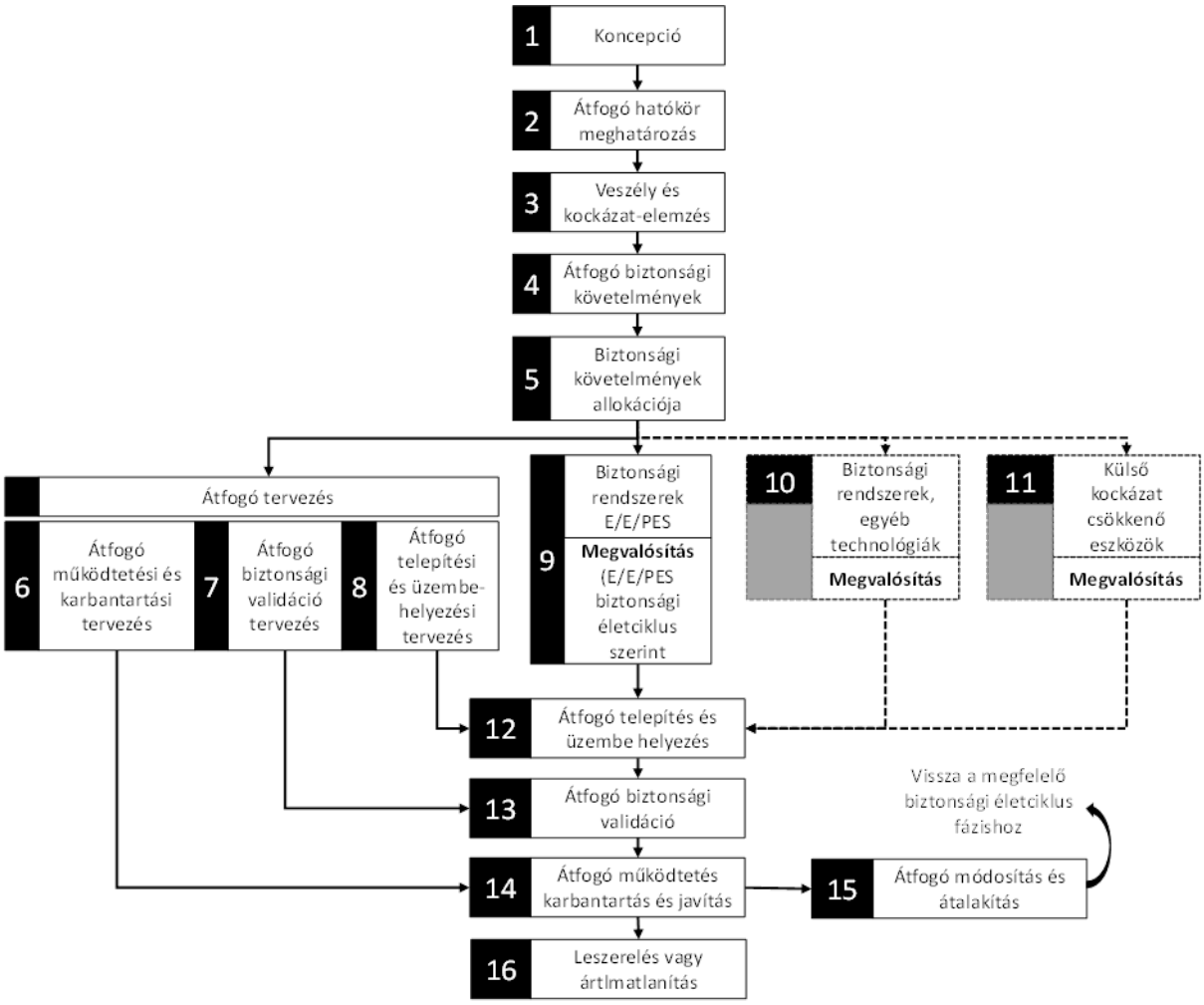
2.3. ábra. Műszaki kockázatmenedzsment folyamata

Bemenetek: A kockázatmenedzsment tipikus bemeneti dokumentumai:

- **Kockázatkezelési terv és politika (Plans and Policies):** Kockázatkezelési terv, a kockázat értékelésének követelményrendszere, a rendszerfejlesztés elvárt folyamata, adatai, elvárt követelmények cél- és határértékei.
- **Műszaki adatok (Technical Inputs):** Teljesítmény kritériumok, számba vehető lehetőségek, döntési változók és azokra vonatkozó korlátok, követelmények, tervezési alapértékek.
- Az alternatív megoldások kockázatelemzéséhez szükséges bemenetek: Tervezési információk, tapasztalati tudás.

2.2 Kockázatmenedzsment életciklus az IEC 61508 szerint

A baleseti okok statisztikája azt mutatja, hogy a balesetek okainak jelentős része már a termék tervezése és gyártása során beépült a termékbe. E felismerés is azt sugallja, hogy a hiba és a megkívánt biztonsági szint fenntartása megelőzése a termék teljes életciklusára kell, hogy vonatkozzon. E fejezet célja, hogy az IEC 61508 szabvány szerint áttekintse az életciklus szemléletű elemzés legfontosabb tevékenységeit. A szabvány szerinti kockázatmenedzsment 16 lépésből álló tevékenységeinek kapcsolódásait az alábbi ábra mutatja.



2.4. ábra. Az IEC 61508 szabvány szerinti életciklus modell.

A módszertan első ténylegesen kockázatelemzéshez kötődő harmadik lépése **az előzetes veszély és kockázatelemzés** [Preliminary Hazard Analysis] melynek célja a veszélyhelyzetek feltárása. E lépés során definiálandók azon meghibásodási lehetőségek melyek balesetekhez vezethetnek. Például feltárandó, hogy egy fékrendszerben milyen meghibásodások fordulhatnak elő és ezen meghibásodások adott szituációkban – pl. a jármű nagy sebessége esetén - milyen baleseteket idézhetnek elő. A negyedik lépés e veszélyhelyzetekhez kapcsolódó általános biztonsági követelmények meghatározását jelenti. Az ötödik lépés célja, hogy az általános biztonsági követelményeket hozzárendelje az adott műszaki részrendszerhez, folyamathoz, pontosabban az ahhoz tartozó veszélyhelyzetekhez, például a fékerő hiányából származó veszélyhelyzetek kezelésére vonatkozó követelményeket a fékrendszerrel szemben fogalmazzuk meg.

Az életcikust átfogó tervezési tevékenységet a 6-8 folyamatlépések fogják össze. A hatodik tevékenységelem a rendszer installálásával, működtetésével és karbantartásával kapcsolatos elvárások megfelelését biztosító tervezési tevékenységet takarja. Ilyen kérdés például, annak meghatározása, hogy milyen gyakran kell a fékrendszert karbantartani. A hetedik lépés a biztonsági rendszer validálásának (ellenőrzésének) rögzítését jelenti, mely példánk kapcsán arra a kérdésre keresi a választ, hogy a miként biztosítsuk, hogy fékrendszerünk a karbantartások és ellenőrzések közti időintervallumban is kellően robusztus, megbízható legyen. A nyolcadik elem a rendszer átadásával, üzembe helyezésével kapcsolatos elvárásokat rögzíti. Erre a lépésre egy vegyipari üzem

átadásával, indításával kapcsolatos előírások rögzítése a kézenfekvő példa, mely azt is illusztrálja, hogy a IEC 61508 szabvány kialakulását a folyamatipar a járműiparnál jelentősebben befolyásolta.

Magukat a biztonságkritikus rendszer tervezésével kapcsolatos feladatokat a 9-11 lépések tartalmazzák.

A biztonságkritikus rendszerek fejlesztésének alapja olyan biztonsági funkciók fejlesztése melyek biztosítják, hogy az adott részrendszer ne járulhasson hozzá a nem megfelelő biztonságú …. azaz biztosítják az adott SIL érték elérését. Azt a részrendszert, amely az adott biztonsági funkció megvalósításához, azaz az adott biztonsági szint eléréséhez szükséges Safety-Related System (SRS)-nek azaz biztonsági rendszernek hívjuk. A kilencedik és tízedik lépések e rendszerek tervezésével, elemzésével és implementálásával foglalkoznak. Az E/E/PE komponenseket tartalmazó rendszerekre a kilencedik, az az ilyen elemeket nem tartalmazó részrendszerekre a tizedik lépés érvényes.

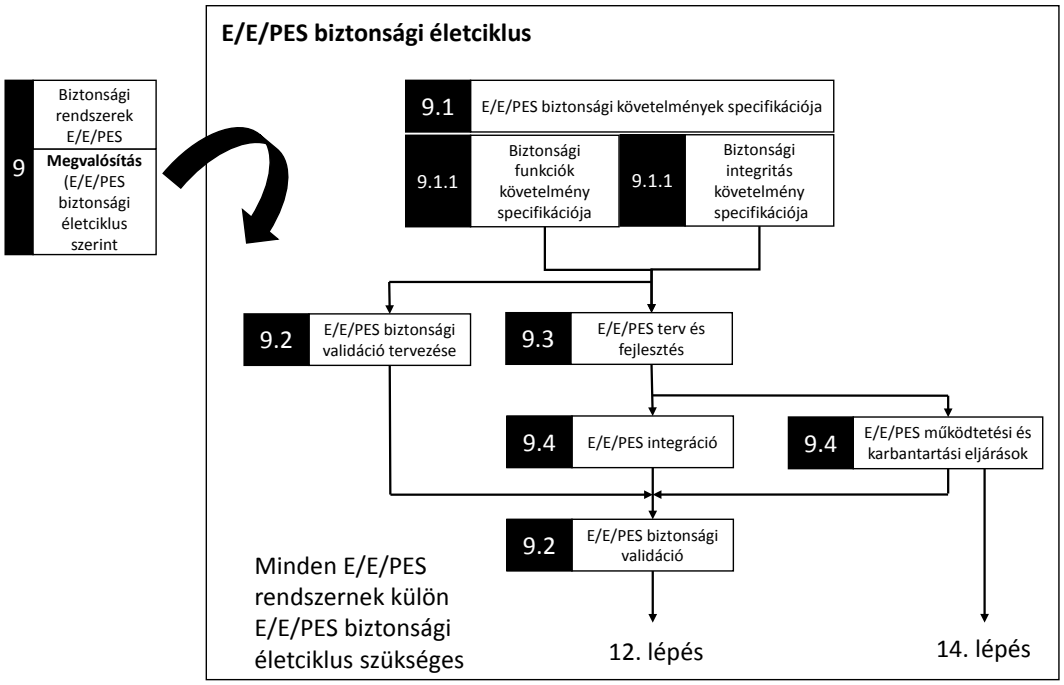
Az IEC 61508 szabvány elsősorban az E/E/PE komponensekre fókuszál, így a kilencedik lépést további részlépésekre osztja.

A szabvány azt is kezeli, hogy a kockázat csökkentésének a biztonsági funkciók fejlesztésén kívül más eszközei is vannak. Példánkat követve például a jármű sebességének korlátozása szintén alkalmas a fékrendszer esetleges meghibásodásával járó kockázatok csökkentésére. Az ilyen jellegű külső kockázatcsökkentő eszközökkel kapcsolatos előírásokat a 11. elem tartalmazza.

A további lépések (12.-16.) alkalmazása a rendszer építését követő, a rendszer telepítéséhez, üzembe helyezéséhez, validálásához, karbantartásához kötődő előírásokat rögzítik.

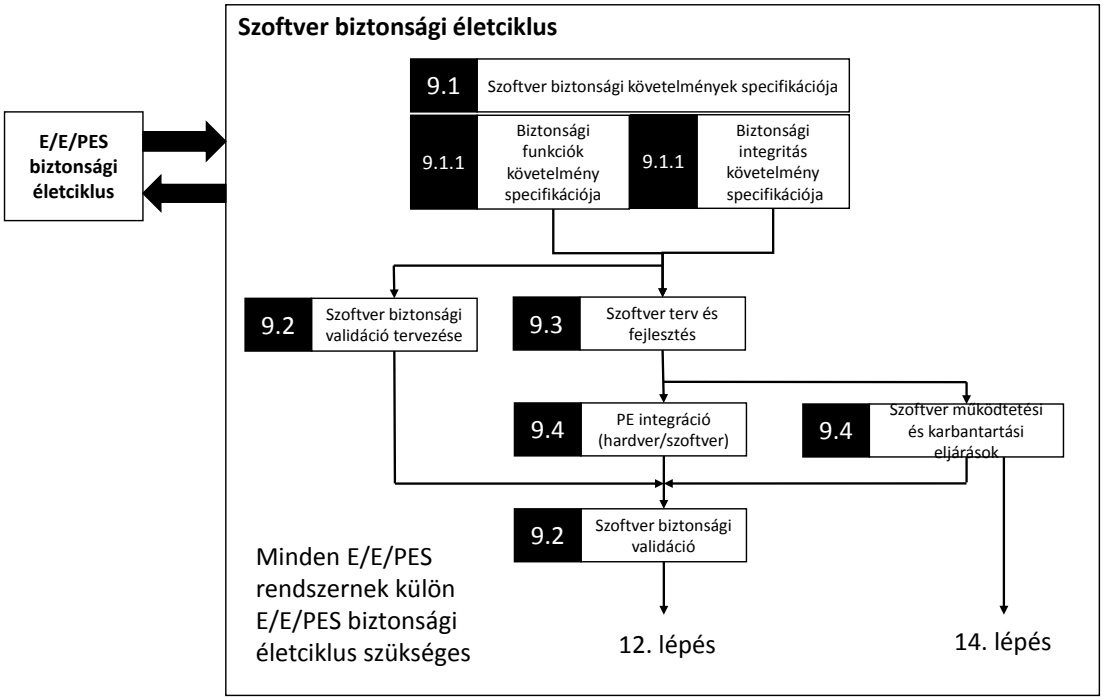
Gyakran előre látható, hogy a működtetés során, illetve a fejlesztést és gyártást követően rendszer módosítása, illetve módosított környezetben való alkalmazása szükséges. Fékrendszeres példánk esetében például elképzelhető, hogy a jövőben az érintett járművek súlya, teljesítménye növekedni fog, így a fékrendszer teljesítményével kapcsolatos elvárások is növekedhetnek. E helyzethez kapcsolódó előírásokat a 15. lépés rögzíti. A leszereléssel, ártalmatlanítással kapcsolatos 16. pontban rögzített tevékenységek a járműiparban sem elhanyagolhatók, gondoljunk csak a gumi, akkumulátor, hulladékok környezeti vonatkozású veszélyeire.

IEC 61508 szabvány az E/E/PE (rész)rendszerek életciklusával kapcsolatban is részletesebb, ugyanakkor az általánosan alkalmazható előírásokat rögzít a kilencedik lépésben (lásd alábbi ábra).



2.5. ábra. Az IEC 61508 szabvány az E/E/PE (rész) rendszerek életciklusával kapcsolatos tevékenységei.

A szabvány a szoftver komponensek elemzésére vonatkozó előírásokat is tartalmaz. Ezek közül külön a 9.4-es integrálási lépés emelendő ki, a részrendszerek egymáshoz illesztésével kapcsolódó kérdések kapcsán a hardver és szoftver komponensek integrációjával foglalkozik, pl. annak a kockázatnak az elemzésével, hogy a kód megfelelő működést garantálja-e az adott célhardveren.



2.6. ábra. Az IEC 61508 szabvány az szoftver elemek életciklusával kapcsolatos tevékenységei

Nagyon fontos kiemelni, hogy ez a biztonsági életciklus séma legfontosabb célja, hogy útmutatóként szolgáljon a kockázatmenedzsment tevékenységhez, illetve annak dokumentálásához. Ez az útmutató tehát nem csak olyan szempontból fontos, hogy felhívja a figyelmet, hogy a fejlesztés és az

alkalmazás során milyen kockázatmenedzsmenthez köthető tervezési, elemzési, monitoring feladatok vannak, hanem ellenőrzési listaként is szolgál, biztosítva azt, csak indokolt és dokumentált esetben maradhasson ki elemzési, tervezési lépés, azaz csak olyan esetben, melyhez kapcsolódóan az elemzések nem mutattak ki kezelendő nem megengedhető kockázatot.

2.3 Kockázatmenedzsment az ISO 26262 szabvány szerint

Az IEC 61508 szabvány elsősorban egyedi gyártással / kis számban készülő technológiákkal foglalkozik, olyan esetekkel, amikor a biztonsági validálást is elvégzik és rendszeren megismétlik. Ezzel szemben az ISO 26262 szabvány tömegtermeléssel előállított 3500 kg-nál könnyebb közúti járművekre vonatkozik. Ebben az esetben a biztonsági validálást a fejlesztés során végzik el. Az IEC 61508 a „szabályozott folyamat/berendezés" modelljére épül, amelyben lehetőség van a rizikócsökkentést szolgáló eszközök alkalmazására. Az ISO 26262 a „biztonságosra tervezett rendszer" modelljét alkalmazza, azaz azzal a megközelítéssel él, hogy a biztonságnak be kell épülnie a rendszerbe, azaz a szabályozási és biztonsági funkciók nem, vagy csak nagyon nehezen választhatók szét. E szabvány szerint a kockázat meghatározása magában foglalja a közlekedési szituáció összes összetevőjét, így az autó vezetőjét és a szituációban érintetteket is.

Az ISO 26262 életciklus-modell erőssége, hogy a biztonsági menedzsmentre és a biztonsági kultúrára helyezi a hangsúlyt, ugyanis nagy komplexitású rendszerek esetén a balesetek inkább a szervezet működésével, kultúrájával, azaz a tervezési, gyártási és működtetési tevékenységgel kapcsolatos faktorok következményei.

Elfogadhatatlan szint	**Megfelelő biztonsági kultúra**
Felelősség nem nyomon követhető.	A folyamat biztosítja a biztonsággal kapcsolatos döntések követhetőségét.
Költség és határidő elsőbbséget élvez a biztonsággal és minőséggel szemben.	(Funkcionális) biztonság a legmagasabb prioritással bír.
Biztonsággal kapcsolatos reaktív hozzáállás (széleskörű tesztelés a termékfejlesztés végén; menedzsment csak akkor avatkozik be, ha probléma van).	megelőző és reflektáló hozzáállás (biztonsági és minőségi kérdéseket a termék életciklusának lehető legkorábbi fázisában felismerik és megoldják).
Nincsenek szisztematikus folyamatos fejlődési ciklusok.	Minden folyamatba beépül, annak része a folyamatos fejlődés.

A jegyzet tartalmi keretei nem teszik lehetővé a szabvány előírásainak részletes ismertetését.

A következő alfejezetben a járműiparban széles körben alkalmazott meghibásodásmód- és hatáselemzési technikát mutatjuk be, mint egy olyan technikát, amely sikeresen támogatja a szisztematikus és folyamatos fejlesztésen alapuló kockázatmenedzsment tevékenységet.

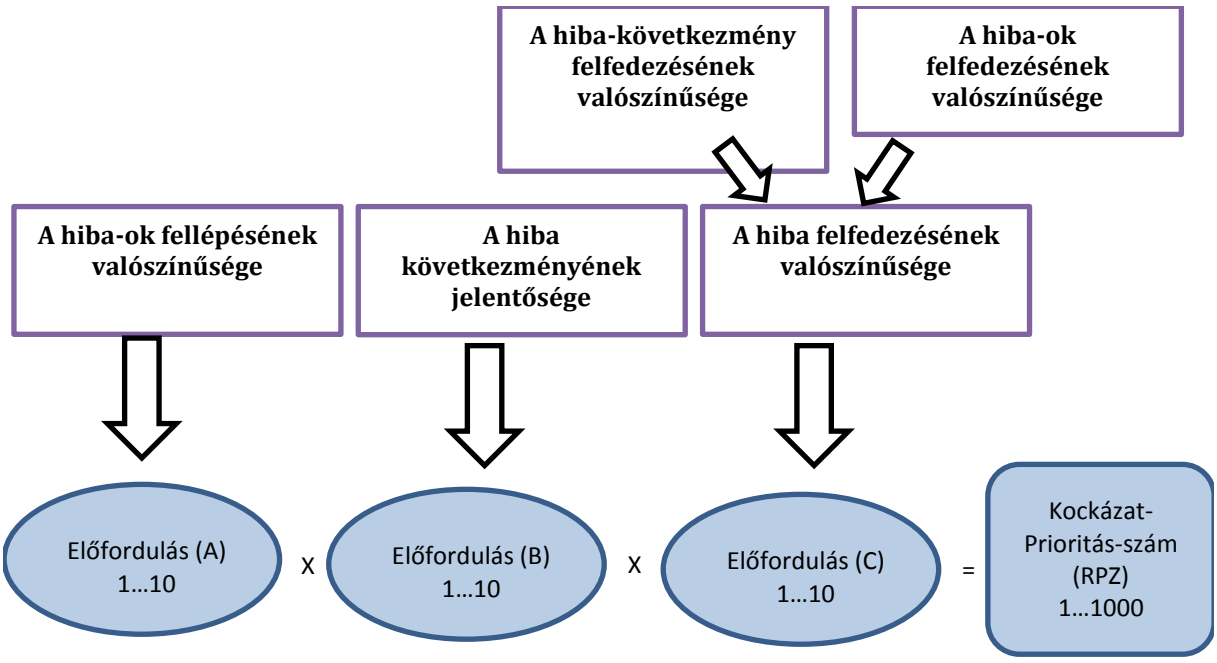
2.4 Meghibásodásmód és –hatás elemzés (FMEA)

Az FMEA (Failure Mode and Effect Analysis – Hibamód- és hatáselemzés) egy tervező, fejlesztő és dokumentációs módszer, amellyel a termékek vagy folyamatok minőségének és megbízhatóságának folyamatos fejlesztése hatékonyan támogatható. Az FMEA olyan a kockázatok számszerűsítését is lehetővé tevőtechnika, amellyel módszeresen azonosíthatók az egyedi komponens hibamódok következményei.Az eljárást az MSZ EN 60812:2006 „A rendszer-megbízhatóság elemzési módszerei. A hibamód- és hatáselemzés (FMEA) eljárása" szabvány rögzíti. Az eljárás célja az összes lehetséges hiba, azok hatásainak, okainak és ellenőrzéseknek a feltárása és súlyozása. A veszélyesnek ítélt

hibákra meg kell keresni azok megelőzésének, feltárásának módját is. Az induktív elemzési módszer alapja a „mi van, ha...?” típusú kérdés. Az FMEA legfőbb jellemzője a rendszer fontosabb részegységeinek, illetőleg komponenseinek vizsgálata abból a szempontból, hogy mi a hibás állapotba jutás módja (a hibamód), és milyen hatást gyakorol a hibamód a rendszerre (a hibamód-hatás). Az FMEA „lentről-felfelé” irányuló megközelítés, mely egyesével veszi figyelembe a komponensek hibamódjainak következményeit. Fontos megjegyezni, hogy az FMEA készítés során minden egyes meghibásodást a többi meghibásodástól független eseménynek tekintünk. A vizsgálat szempontjából érdektelen, hogy a vizsgált hiba valójában előfordult-e, vagy csak elvileg lehetséges. A meghibásodások leírását az elemzők felhasználhatják ahhoz, hogy meghatározzák a rendszer tervének vagy egy gyártási, üzleti, netán szolgáltatási folyamat javítása érdekében szükséges változtatásokat. A módszert a folyamatos fejlesztés jegyében alkalmazva rendszeresen ellenőrzik a kockázatcsökkentésre vonatkozó javaslatok megvalósítását és új javaslatokat készítenek a mindenkori legsúlyosabb láncolat megkeresésére és megszüntetésére. Az FMEA sikeres alkalmazásának egyik legfontosabb tényezője, hogy egy soha véget nem érő folyamat. Az elemzés a hangsúlyt a megelőzésre helyezi, igyekszik feltárni egy termék/folyamat lehetséges hibáit. A módszer helyes alkalmazása esetén egy interaktív, állandó folyamat, amely egyre tökéletesebb terméket és folyamatot eredményez.

Az FMEA általában leíró jellegű elemzést tesz lehetővé, melynek kerete, hogy a kockázatérékeléshez szükséges információt adattáblázatba gyűjtik, vagy munkalapra vezetik. Az elemzés kulcsfontosságú kimenetei a veszélyhelyzetre vonatkozó kockázati indexek (Risk Priority Number, RPN), melyek alapján értékeljük a vizsgált konstrukciót ill. folyamatot. Az RPN egy komplex mutató, mely egyaránt tartalmazza a gyártó és a vevő szempontjait is. Értékét a három pontszám (súlyosság, előfordulás, felderítés) szorzata adja (lásd alábbi ábra):

$$RPN = súlyosság \times előfordulás \times felderítés \tag{2.1}$$



2.7. ábra. FMEA értékelési rendszere, a kockázat-prioritás-szám meghatározásának módja

Súlyosság mutatószám a hibák bekövetkezésekor a hibák következményeit értékeli, elsősorban a vevő szempontjából, 1-től 10-ig terjedő skálán pontozással (lásd alábbi táblázat).

Pontszám	Meghatározás
1	A hibát a felhasználó valószínűleg fel sem fedezi, a hiba hatása a felhasználóra nézve jelentéktelen.
2-3	A hibát a felhasználó valószínűleg érzékeli, de a gyártmány működését nem vagy csak kis mértékben befolyásolja.
4-6	A hiba észrevehető mértékben fordul elő, a működést zavarja, a felhasználó a gyártmánnyal elégedetlen lehet, de a termék alapvetően működőképes.
7-8	A termék nem működik, vagy alapvetően funkciói hiányosak, a felhasználó a termékkel elégedetlen.
9-10	A termék a felhasználóra veszélyes, a környezetre ártalmas, sérti a hatósági előírásokat

Ha egy hiba hatásra az értékelés 1, akkor arra a hibahatásra nem kell további elemzést végezni. Magas osztályzatok esetén a hiba hatásának súlya kompenzálható, vagy csökkentheti a termék konstrukciójának felülvizsgálatával. Pl. az ún. „durrdefekt" hatása csökkentheti azzal, ha a gumi lassan ereszt csak le, vagy a biztonsági öv alkalmazása csökkenti a jármű ütközése során fellépi hatás súlyosságát.

Előfordulás mutatószám 1-től 10-ig terjedő skálán pontozással azt jellemzi, hogy mekkora annak a valószínűsége, hogy egy adott hibaok bekövetkezik és meghibásodást okoz (lásd alábbi táblázat). Az FMEA-t készítő team-nek 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. Az alábbi táblázat irányelveket tartalmaz a gyakoriság kiértékeléséhez, amelyek alkalmazása javasolt.

Pontszám	Relatív gyakoriság	Meghatározás
1	0,00002-0,00005	A folyamat szabályozott, a hiba előfordulásának valószínűsége igen kicsi
2-5	0,00005-0,005	A folyamat a szabályozottság határesetében van, hibák kis számban előfordulhatnak (előfordulnak)
6-8	0,005-0,05	A folyamat szabályozatlan, hibák nagy számban előfordulnak
9	>0,05	A hiba előfordulása gyakorlatilag elkerülhetetlen
10		A hiba biztosan bekövetkezik

Járműiparban alkalmazott értékelési rendszerre példa az alábbi táblázat.

Hiba előfordulás valószínűsége	**Lehetséges meghibásodási arányszám**	**Pontszám**

Nagyon magas: Állandó jelleggel jelen lévő hiba	hibák száma ≥100 db 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 5 db 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

Felderítés (azaz a hiba rejtve maradásának valószínűsége): annak az értékelése, hogy a jelenlegi ellenőrző intézkedések, azaz azok a vizsgálatok, ellenőrzések, melyeket jelenleg használnak az adott hibamód vagy hibaok megelőzésére, feltárására, pl. laborvizsgálatok, auditok, ellenőrzések, tesztelések mennyire hatékonyak. Ezt a szempontot is szintén 1-től 10-ig pontozzák, annak a valószínűségét megbecsülve, hogy az adott vizsgálati eljárás nem szűri ki a hibaokokat ill. a meghibásodásokat (lásd alábbi táblázat).

Pontszám	Relatív gyakoriság	Meghatározás
1	0,00002-0,00005	Annak valószínűsége, hogy a hibás termék átvételre kerül, gyakorlatilag nulla. A hiba nyilvánvaló vagy az ellenőrzés 100%-os

2-5	0,00005-0,005	Annak valószínűsége, hogy a hibás termék átvételre kerül, igen kicsi. A hiba nyilvánvaló, vagy az ellenőrzés 100%-os esetleg statisztikai, de nagy minták vételén alapul.
6-8	0,005-0,05	A hibát „közepes” valószínűséggel fedezik fel. Az ellenőrzés statisztikai, kis minták alapján. Az esetleges 100%-os ellenőrzés felszínes, pl: szemrevételezés.
9-10	>0,05	A hibás termék nagy valószínűséggel átvételre kerül; ha a hiba rejtett, a terméket nem ellenőrzik (pl: ez nagyon költséges vagy lehetetlen) ill. a statisztikai ellenőrzés mintái nagyon kicsik.

Az RPN értékeket sorba rendezve a legmagasabb pontszámot kapott problémákra tudunk koncentrálni, azaz megkapjuk melyek azok a veszélyhelyzetek melyek kapcsán javító intézkedéseket kell tenni.

Az RPN érték alapján a következő döntések születhetnek:

- RPN < 40 A kockázat elfogadható, nincs szükség intézkedésekre
- RPN > 100 A kockázat nem elfogadható, intézkedés szükséges
- RPN < 40 < 100 Bizonytalan kockázatbecslés, az értékelés felülvizsgálata

Az RPN értékétől függetlenül a gyakorlatban külön figyelmet szentelnek azoknak a hibáknak, melyek súlyosság pontszáma magas.

Miután a hibafajtákat az RPN alapján rangsoroltuk, javító intézkedéseket kell meghatároznunk a legmagasabb értékű hibákra ill. a kritikus jellemzőkre. A javító intézkedések célja, hogy csökkentsük az RPN faktor értékét. A javítási intézkedések részeként meg kell nevezni az adott intézkedés végrehajtásáért felelős személyt és a határidőt. A javító intézkedések bevezetése után ismételten meg kell határozni az RPN értékét.

A hibamód és hatáselemzés általánosan alkalmazható rendszerekre, alrendszerekre, berendezésekre, funkciókra, (technológiai) eljárásokra, és folyamatokra.

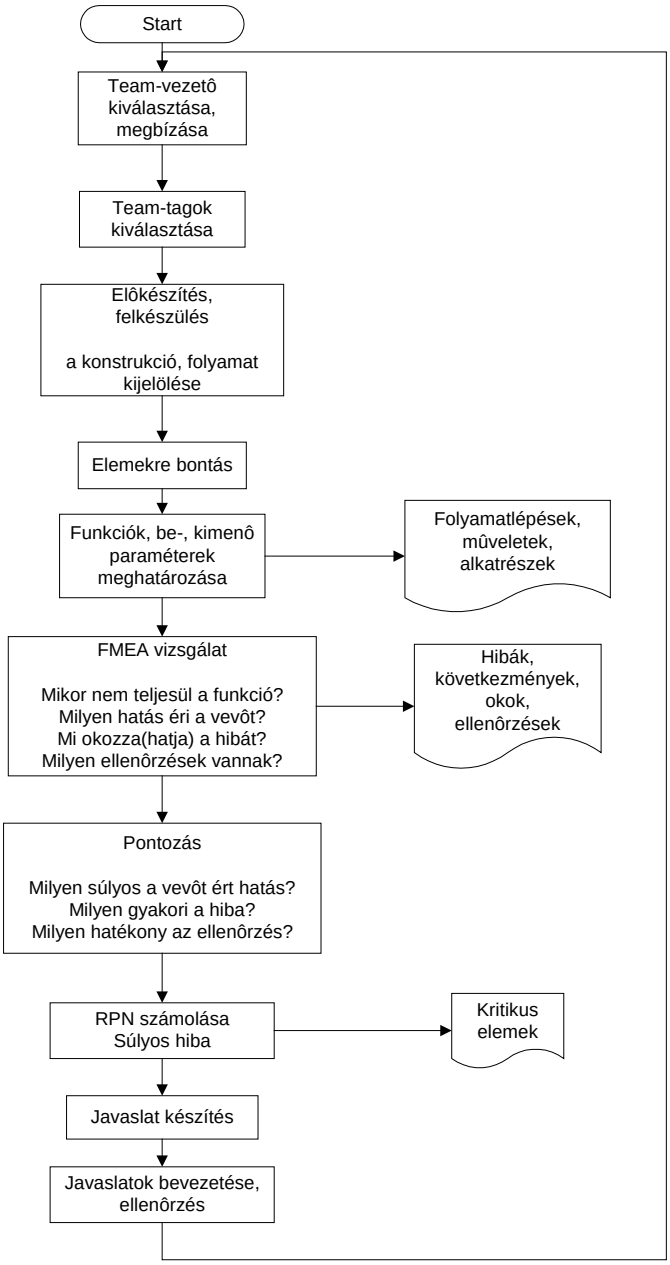
A **konstrukciós, tervezési** (design) FMEA-t a termékkonstrukció elemzésére, a tervezésből eredő hibák és hibalehetőségek feltárására alkalmazzák, azaz mielőtt a termék gyártása megkezdődne.

A **folyamat, gyártási** (process) FMEA-t a gyártási és szerelési folyamatok elemzésére, a gyártás során fellépő hibák, hibalehetőségek feltárására és megszüntetésére alkalmazzák. A folyamat FMEA figyelembe kell, hogy vegye a gyártási technológiát, az ellenőrzési lépéseket, és a logisztikát. A folyamat FMEA a konstrukciós FMEA-ra épüljön.

Ahogy az alábbi példák illusztrálják, FMEA-ra készítését, frissítését szervezeti változások, termék-változások, új folyamatok, folyamat-/ termék-áttelepítések tehetik szükségessé,

- Új termék, technológia vagy gyártófolyamat. Az FMEA ebben az esetben a teljes termékre, technológiára és gyártófolyamatra kell, hogy kiterjedjen.
- Meglévő termék vagy gyártófolyamat módosítása. Feltehetően létezik már korábban elkészített FMEA elemzés, így a módosítás esetleges hatásaira kell figyelmet fordítani.
- Meglévő termék vagy folyamat új alkalmazása vagy új gyártási környezetbe helyezése. Feltehetően már létezik korábbi FMEA. Ebben az esetben a megváltozott környezetre, helyszínre vagy alkalmazásra kell összpontosítani a figyelmet.

Az FMEA készítésének a folyamata a következő ábrán látható. Fontos megemlíteni, hogy a fenti séma teljes egészében lefedi a kockázatmenedzsment előző fejezetben vázolt folyamatát.



2.8. ábra. Az FMEA készítésének folyamata.

Az FMEA forgatókönyv jellegű segítséget ad a lépésekhez, de nem helyettesíti a szakmai ismereteket, melyek általában műszaki-tudományos ismereteket és a konkrét gép, rendszer konstrukciós, technológiai, alkalmazás, stb. ismereteit jelentik. Ezen ismeretigény miatt javasolt a multidiszciplináris csoport kialakítása és csoportos alkotó módszerek alkalmazása, annak ellenére, hogy az FMEA tevékenységet az alaptevékenységért felelős mérnök kezdeményezi (termék-tervezés, technológia).

4	Típus év/jármű:		/5/			Határidő:				/6/	FMEA dátum (eredeti):			(felülvizsgálva):							
5	Team:								/8/												
6																					
7			/12/		/13/		/15/			/17/				Tevékenységek eredménye /22/							
8	Folyamat Funkció /9/ Követelmények	Potenciális hiba /10/	A hiba potenciális hatása(i) /11/	Jelentőség	Minősítés	A hiba potenciális oka(i)/ mechanizmusa(i) /14/	Előfordulás	Jelenlegi megelőzési folyamat /16/	Jelenlegi ellenőrzési folyamat /16/	Észlelés	RPN /18/	Javasolt intézkedések /19/	Felelős, határidő /20/	Bevezetett intézkedés /21/	Jelentőség	Előfordulás	Észlelés	RPN			
9																					
10																					
11																					
12																					
13																					
14																					
15																					
16																					
17																					
18																					
19																					
20																					
21																					
22																					
23																					
24																					
25																					
26																					
27																					
28																					

FMEA – dokumentum kitöltése

Az FMEA készítése során első lépésként azonosítani kell a termék részegységeit/alkatrészeit, a folyamat lépéseit (műveleteit) és azok elvárt funkcióit. E lépésben összesíteni kell a vevő elvárásait, igényeit. A dokumentálás megkönnyítése érdekében az elemzést célszerű egy előre elkészített formanyomtatványon, táblázaton végezni. Egy tipikus FMEA űrlap látható az előző táblázatban.

FMEA száma: Az FMEA dokumentum számát írjuk be ide a későbbi azonosítás és nyomonkövethetőség érdekében.

Rendszer, Alredszer, 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 team tagjainak el kell dönteni, hogy mi alkot rendszert, alrendszert, vagy mi az alkatrész a team specifikus tevékenysége szempontjából. A határok meghúzása a rendszer, alrendszer vagy alkatrész szempontjából önkényes, és az adott esetben ez mindig a team döntésén múlik.

A rendszer FMEA tárgyköre: A rendszer úgy tekintheti, mint több különbözi alrendszerből felépített egység. ezeket az alrendszereket az esetek többségében különbözi team-ek tervezik. Tipikus példák arra, amit rendszer FMEA-val lehet lefedni: szerelt műszerfal, erőátviteli rendszer, kocsi belső tér stb..

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.

1) **Tervező** Az elemzett egység tervezéséért felelős személy, osztály vagy team megnevezése. Ha alkalmas, akkor tüntessük fel a szállító nevét.
2) **Készítette** Az FMEA elkészítéséért felelős személy neve, telefonszáma, az érdekelt szervezeti egység (osztály, vállalat) megnevezése.
3) **Modell év / Program** Az elemzett egység elhatározott felhasználási területe illetve modell éve írandó ide, ha ismert.
4) **Kiadás dátuma** Az FMEA első esedékességének, kiadásának dátuma, ami nem lehet későbbi mint a termék kibocsátási, jóváhagyási dátuma.
5) **FMEA dátuma** Az FMEA első komplett megvalósításának és a legutóbbi felülvizsgálatának dátuma.
6) **Alap team** Azoknak a team tagok nevének felsorolása, akik hatáskörrel és felelősséggel rendelkeznek a feladat azonosítására és végrehajtására.
7) **Egység / funkció** Írjuk be az egység nevét és egyéb vonatkozó információkat (pl. 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, mérheti információkat, arra a környezetre, amelyben a terméknek funkcionálnia kell (hőmérsékletű tartomány, nyomás, páratartalom, élettartam).

Ha az egység több funkcióval rendelkezik különbözi lehetséges meghibásodási módokkal, soroljuk fel mindegyik funkciót.

8) **Lehetséges meghibásodás mód** 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 elői. A lehetséges meghibásodások megfogalmazására „fizika", technikai terminológiát alkalmazzunk, és ne a tünetek leírását, ahogy ezt esetleg a vevői megfogalmazza.
9) **Lehetséges meghibásodás mód** 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 elői. A lehetséges meghibásodások megfogalmazására „fizika", technikai terminológiát alkalmazzunk, és ne a tünetek leírását, ahogy ezt esetleg a vevői megfogalmazza.
10) **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 team ismereteinek megfelelően.
11) **Hiba hatásának súlyossága, jelentősége** A súlyosság egy adott hiba esetében a legsúlyosabb hatás számmal történi osztályozása. A súlyosság egy relatív értékelés az adott FMEA-n belül. A súlyosság kiértékelésére adott osztályzat csak a termék konstrukciójának megváltoztatásával lehetséges.
12) **Osztályozás** Ez az oszlop használható arra, hogy osztályozzuk a speciális termék jellemzőket (pl. 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 team úgy találja, hogy ez segítséget nyújt a további munkához, vagy a helyi vezetés ezt igényli. A speciális termék és folyamat jellemzik azonosítására szolgáló szimbólumokat és azok használatát az egyes vállalatoknak kell meghatározni, és erre vonatkozó egységes előírások nem találhatóak ebben a dokumentumban.
13) **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.

14) **Előfordulás, gyakoriság** A gyakoriság azt a valószínűséget fejezi ki, hogy egy megadott hiba ok 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 érheti el az előfordulás valószínűségének csökkenése. A hiba ok vagy mechanizmus előfordulási gyakoriságán becslése egy 1-10 skálán történik. **Ennek a kiértékelésnek az elvégzéséhez javasolt a következi kérdések áttekintése:**

    a. Milyen értékesítés utáni szerviz és használati tapasztalatok állnak rendelkezésünkre hasonló termékre?
    b. A jelenlegi alkatrész egy régi vagy hasonló egy régi alkatrészhez?
    c. Milyen jelentős változások vannak egy korábbi termékhez képest?
    d. Az új alkatrész radikálisan eltér a korábban alkalmazottól?
    e. Az alkatrész teljesen új?
    f. Az alkatrész alkalmazása megváltozott?
    g. Vannak környezeti változások? Ha igen mik azok?
    h. Végeztek műszaki vizsgálatokat (pl. megbízhatóság), hogy felmérjék a várható hiba előfordulási valószínűséget?
    i. Léptettek életbe a hiba előfordulását megelőzi 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.

15) **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, biztonságosság pl. túlnyomásra kiolvadó szelep, vizsgálatok, matematikai elemzések, gyárthatóság kiértékelés, prototípus vizsgálatok, országúti vizsgálatok stb.) azok az intézkedések, melyeket hasonló termékek esetében jelenleg alkalmaznak. A team-nek mindig törekednie kell arra, hogy a jelenleginél hatékonyabb módszereket azonosítsanak, mint pl. új labor vizsgálat, új modellezőalgoritmus, stb.

16) **Jelenlegi szabályozás** 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: Detektálja, 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 ill. mechanizmusát észleli.

    A termék FMEA formátum ebben a kézikönyvben két oszlopot tartalmaz a jelenlegi szabályozás számára. (külön oszlop a megelőzi és külön oszlop a detektáló intézkedésekre), hogy segítse a team 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.

17) **Észlelés, detektálás** A detektálás egy 1-10 skálán végzett osztályozás, ami a legjobb felsorolt detektálási módszer hatásosságát tükrözi. A detektálás pontszáma egy relatív szám és csak az adott FMEA-n belül érvényes. Az adott pontszám csökkentése érdekében hatásosabb megelőzési, ellenőrzési, detektálási módszereket kell bevezetni.
Javasolt kiértékelési szempontok: A team-nek 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 leheti leghamarabb életbe kell léptetni a fejlesztési munka során.
18) **Kockázati tényező (RPN)** A kockázati tényezi az eddig megállapított, egymástól független kockázati tényezőkből -a jelentőség, a előfordulás és a észlelés határozható meg.
$$RPN = (A) \times (B) \times (C)$$
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 becslésébe.
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 rendelkezi meghibásodásokra kell alkalmazni, vagy azokra, amelyeket a team meghatároz. Minden javító intézkedésnek az a célja, hogy csökkentse a meglévő kockázatokat a következi sorrendben: a hiba hatásának súlya, az gyakorisága, a detektálás hatásossága.
20) **Javasolt intézkedés(ek)** 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 / megelőzi intézkedéseket kell alkalmazni a következmények elkerülése érdekében a hiba okok megszüntetésével, csökkentésével vagy ellenőrzésével.
Miután speciális intézkedéseket vezettek be a súlyos hatású kockázatokra, 9 – 10 értékek, a team a többi meghibásodásra fogalmaz meg javító intézkedéseket a súlyosság, előfordulási gyakoriság csökkentésére ill. a észlelés hatásosságának növelésére.
21) **Felelős / határidő** Ebbe az oszlopba írjuk be az intézkedés bevezetéséért felelős személy vagy szervezet nevét, és a tervezett határidőt.
22) **Bevezetett intézkedés** Miután az intézkedést bevezették, ebbe az oszlopba írjuk be röviden megfogalmazva a hatályba lépés dátumával.
23) **Eredmény** A meghatározott és bevezetett intézkedés kiértékelését is el kell végeznünk a hiba hatás súlyossága, az előfordulás gyakorisága, és a detektálás hatásossága 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.

FMEA -Utógondozás (Follow up)

A megfelelő javító intézkedések bevezetését és nyomon követését nem lehet túlhangsúlyozni. A bevezetett intézkedéseket minden érintett területtel közölni kell. Egy bármilyen alaposan végiggondolt és gondosan elkészített FMEA csak nagyon kis értéket képvisel bevezetett javító ill. 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, beleértve 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, pl.

- A műszaki rajzok, folyamatleírások és munkautasítások átnézése, hogy tartalmazzák-e a javasolt intézkedéseket.
- A megfelelő dokumentációk jóváhagyása a termékre, folyamatra, munkautasításokra vonatkozóan.
- A megfelelő termék és folyamat FMEA-k áttekintése, speciális FMEA alkalmazások, „control plan" átvizsgálások.

A termék FMEA egy élő dokumentum kell, hogy legyen, ami a következőket jelenti:

- Elkészítését a tervezési koncepció alatt, vagy annak véglegesítése előtt kell elkezdeni,
- 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.

Az FMEA tehát alkalmas:

- Rendszer, folyamatok, termékek meghibásodási lehetőségeinek minőségi értékelésére
- Kockázat csökkentésére, költségcsökkentésre
- Gyenge pontok felderítésére, javító intézkedések bevezetésére
- Kiesések elkerülésére
- A konstrukció megbízhatóvá tételére
- Új gyártmányok, gyártási eljárások optimalizálására
- Jobb termékminőség elérésére
- MoC

Előnyei:

- Következetes módszer
- Válság-management helyett kockázat-management
- Számszerűsített kockázat
- Dokumentált tapasztalatok
- Célzott ok-hatás elemzés

Hátrányai:

- Nagy időigény
- Szubjektív kockázatbecslés
- Költségek és a haszon nehezen becsülheti

- Jelentős utógondozást igényel

Az FMEA leginkább ott vált be, ahol a helyzeti veszély mechanikai berendezésből, villamos meghibásodásból, stb. ered, és nem a folyamatok dinamizmusából. (Szemben pl. a HAZOP módszerrel, amely a teljes folyamat elemzésére irányul.)

Az FMEA kiterjeszthető olyan módszerré is, amelyet meghibásodásmód, -hatás és hibakritikusság elemzésének (FMECA) neveznek. Az elemzés célja – az FMEA céljain túl – ama rendszerelemek hibakritikusságának rangsorolása, amelyek személyi sérülést, károkat vagy egyéb rendszersérülést okozhatnak az egyedi meghibásodások következtében. A rendszerelemeket az ártalompotenciájuk szerint rangsorolják azon a skálán, amely a meghibásodás bekövetkezése esetén az egyes elemek által okozható károkat jeleníti meg. Hibakritikusság elemzéssel megtalálhatók azok a rendszerelemek, amelyekre a tervezés és a működtetés során külön figyelmet kell fordítani és külön intézkedéseket kell tenni. A módszer általánosan alkalmazható minden rendszerre, folyamatra, eljárásra vagy azok bármely elemére. Az FMEA és FMECA technikákat az IEC 60812 szabvány mutatja be részletesen.

3 Biztonságkritikus rendszerek

3.1 Meghibásodáshoz kapcsolódó fogalmak

Műszaki kockázatok menedzsmentjének elsődleges célja biztonságkritikus rendszer fejlesztése, azaz az elfogadható kockázatnak megfelelő biztonsági szint elérése.

Egy komplex műszaki rendszer esetén általában a rendszer valamely jellemzőjével szemben a szokásosnál nagyobbak a követelmények. Az ilyen rendszereket **kritikus rendszernek** nevezzük. **A biztonságkritikus rendszer** elsődleges követelménye, hogy ne veszélyeztesse az emberi életet, egészséget és ne okozzon gazdasági vagy környezeti károkat. A biztonságkritikus rendszerek tervezésével és üzemeltetésével szemben támasztott követelmények túlmutatnak a **nem-kritikus rendszerekkel** szemben támasztott követelményeken. A legfontosabb különbség, hogy a biztonságkritikus rendszerek esetében **kiegészítő intézkedések szükségesek a hibák következményinek csökkentésére**. Azokban az esetekben, ahol a következmény súlyossága oly jelentős, hogy a megengedhető kockázati gyakoriság megköveteli, hogy a nem kívánt esemény csaknem elhanyagolgató valószínűséggel következzen be, a megfelelő biztonság eléréséhez hibatűrő rendszerek alkalmazására van szükség.

A hibatűrő rendszerekben nincs egyetlen olyan pont sem, amelynek meghibásodása meghiúsíthatja a rendszer működését, azaz a legfontosabb előírt feladatait bármikor ne tudná végrehajtani. A hibák alacsony szinte tartásához kapcsolódó intézkedések a termék teljes életciklusára ki kell hogy terjednek:

- A hiba okok **elkerülése** kapcsán cél, hogy a fejlesztési tevékenységet olyan körültekintően és szisztematikusan végezzük, hogy az esetleges hibákat megelőzzük.
- A hiba okok **eltávolítása** kapcsán cél olyan HW és SW tesztelési technikák kifejlesztése melyek üzembe helyezés előtt való alkalmazásával háríthatók el a hibák.
- A hibák **detektálása** kapcsán a cél, hogy üzemeltetés során a detektált hibák hatásának időbeni mérséklése céljából a megfelelő beavatkozások elvégzésére alkalmasak legyünk. Ez gyakran a meghibásodott komplex funkció nélküli üzemállapotra történő átállást jelent.

Tekintettel arra, hogy az előzőekben említett hibamenedzselési technikák (elkerülés, eltávolítás, detektálás) kombinációja önmagában soha nem tökéletesen hatékony, e technikák hatékony kombinálása, integrált alkalmazása szükséges.

A funkcionális biztonság elérhető:

- komplexitásra ható fejlesztésekkel
    - a rendszer komplexitásának növelésével, például diagnosztikai funkciók fejlesztésével vagy redundancia növelésével
    - szoftver funkciók növelésével
    - biztonsággal kapcsolatos elektronos/elektronikus rendszerelemek számának növelésével
- vevői igények és végfelhasználói elégedettség fokozott figyelemmel történő kezelésével
    - funkcionális biztonsággal kapcsolatos szabvány szerinti fejlesztéssel
    - igények és megjegyzések módszeres kezelésével
- törvényi szabályozás és szabványok széles körű alkalmazásával.

A fenti szempontok szisztematikus, hierarchikus, integrált és funkcióorientált rendszerfejlesztési tevékenység során érvényesíthetők.

Az integrált hibamenedzselés megfelelő eszközeinek fejlesztéséhez elengedhetetlen a meghibásodási folyamat alapos modellezése.

E modellezés alapja, hogy a hibák bekövetkeztését a hibák hármas szintjével írjuk le.

Az első szint a **hibaok** (fault) nem más, mint az az elsődleges ok, amely esetlegesen összetett hatásláncon keresztül a meghibásodáshoz vezet. A hibaok bekövetkezése lehet véletlenszerű vagy szisztematikus. Véletlenszerű hibák elsődlegesen hardver komponensek esetében jelennek meg fizikai folyamatok eredményeként, míg szisztematikus hibák inkább az emberi tényezőknek, nem megfelelő specifikációnak, kivitelezésnek az eredményeként fordulnak elő. A szoftverhibának szisztematikusak, az a tény, hogy nincs véletlenszerű szoftverhiba a biztonságkritikus rendszer fejlesztését is döntően meghatározza, ugyanis a szisztematikus hibák a fejlesztésben alkalmazott módszerek alapos megválasztásával küszöbölhetők ki.

A véletlen hibák kapcsán egyszeres/többszörös hibáról beszélhetünk, annak függvényében, hogy egymástól függenek-e a meghibásodások (kaszkád-hiba; közösok-hiba). A kétpont-hiba (dual-point failure) olyan meghibásodás, mely két független, közvetlenül egy biztonsági cél megsértését célzó hiba kombinációjának következménye, például az egyik hiba a biztonsággal kapcsolatos elemet érinti, míg a másik hiba biztonsági mechanizmust, mely az adott elemet védi.

A bekövetkezés időtartama szerint tartós vagy átmeneti hiba okokat különböztethetünk meg. Fontos megjegyezni, hogy annak ellenére, hogy a hiba ok átmeneti jelleggel, csak egy rövid időszakra jelenik meg, hatása a lehet tartós.

A második szint a **hiba** (error) szintje az az eseményt jelenti, amikor a hiba ok aktiválódik. Azaz a hiba a műszaki rendszer azon rendszerállapota, amely hibajelenséghez vezet.

Hibajelenség (failure) a hiba azon következménye melynek köszönhetően a rendszer nem képes a megkövetelt funkciók végrehajtására.

A jármű esetében a jármű szintjén (az ISO 26262 szabvány fogalomhasználata szerint a tétel szinten) megjelenő hibajelenség értelmezhető veszélyhelyzetként, míg a komponens szintjén előforduló hibajelenség a tétel (jármű) szintjén gyökérokként (fault) jelenik meg.

(komponens: nem rendszer szintű, logikailag és műszakilag szeparálható elem, azaz a rendszer összetevője).

Működőképesség – túlélési valószínűség (Reliability) Annak a valószínűsége, hogy egy rendszer meghibásodása csak adott időpont után következik be

Rendelkezésre állás (Availability) Adott időpontra vonatkozó működőképesség valószínűsége

Javíthatóság (Maintainability) Adott időpontra a meghibásodott rendszer újra üzembe helyezésének valószínűsége

Biztonság – ellenálló képesség (Safety) a veszélyeztetettségtől mentes állapot valószínűsége

A megbízhatóság vizsgálatot a teljes életciklusra (a berendezés tervezése, a gyártása, és az üzemelése) az IEC 61508 szabvány terjesztette ki, mely számos iparág és alkalmazás számára egységes nyelvezetet és eljárástechnikát ajánl. Az alapfogalmak bevezetésétől, a szakkifejezések definiálásán keresztül, a számítási és intézkedési eljárások áttekintéséig ad az egyes eszközök, valamint az eszközökből felépített rendszerek megbízhatóságára a szakhatóságok számára ellenőrizhető választ.

Az IEC 61508 szabvány szerint az irányított berendezés (EUC – equipment under control) irányító rendszere el kell, hogy különüljön a független vész-, védelmi rendszertől. A két különálló irányítási rendszer eltérő jellegű hibás üzemmódjait sorolja fel az alábbi táblázat.

3.1. táblázat. Meghibásodási üzemmódok.

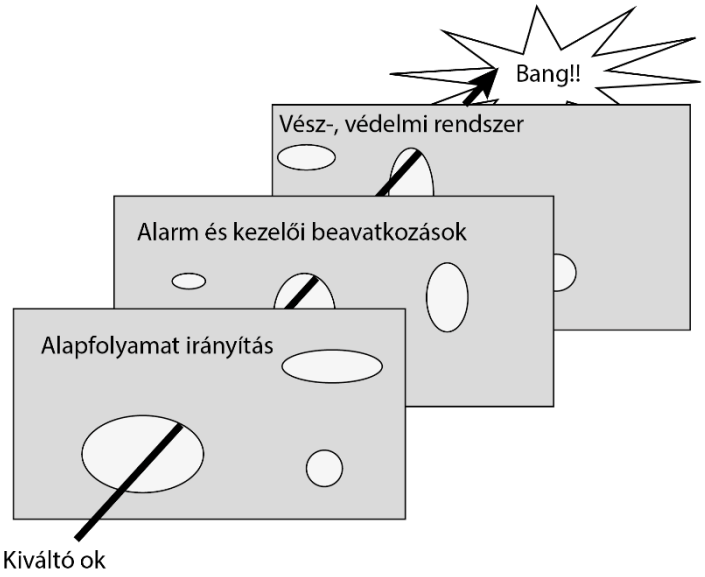
Irányítási rendszer	Vész, védelmi rendszer
A beavatkozó alsó, felső véghelyzetben, vagy kifagyott	**Működtetéskor fellépő hiba (Fail-Danger = Veszélyes hiba)**
Az szabályozó kimenete túl alacsony, vagy túl magas (előjelzés)	**Késleltetett működés (Fail-Danger = Veszélyes hiba)**
A távadó jele, vagy a beavatkozó eszköz reagálása akadozó	**Hamis működtetés (Fail-Safe = Kezelhető hiba)**

A két különálló irányítási rendszer alkalmazását az indokolja, hogy amíg az alapirányításban a hibajelenséget a kezelőszemélyzet általában azonnal észleli, addig a vész, védelmi rendszerek hónapokig, vagy jó esetben akár több évig sem hajtanak végre beavatkozásokat.

Az alapfolyamat irányítás tehát aktív, ezért a rejtett hibák hamar kiderülnek. A kezelő személyzet hamar észleli, ha a berendezés nem megfelelően működik és gyorsan korrigál, elkerülve a nagyobb bajt. A vész-, védelmi rendszer passzív. Szerencsés esetben a kezelő személyzet sohasem észleli működését, így nem veszi észre a baljós előjeleket. Csak az intenzív teszt (úgynevezett proof teszt) és karbantartás biztosítja, hogy e védelmi eszközök szükség esetén megfelelő biztonsággal történő működőképességét. A 90-es évek közepéig a szabványok kategorikusan az alapfolyamat irányítás, és a vész-, védelmi rendszer fizikai szétválasztását írták elő. Manapság, amikor az alapfolyamat irányítása, és a vész-, védelmi rendszer kialakítása jórész programozható eszközökkel történik, és az eszközök egyre megbízhatóbbak, valamint képesek, akár többszörös redundáns működésre számos szakértő felveti a két rendszer integrálhatóságát. A szabvány azonban előírja, hogy a vész-, védelmi rendszer érzékelői és a programozható irányító berendezése fizikailag is független legyen. Ugyanakkor az adatátvitel amennyiben az nem befolyásolja a vész-, védelmi rendszer működését, történhet az alapfolyamat irányítással közös hálózaton.

Az irányítási rendszerek független működésének hasznát az alábbi ábrán vázolt „sajtmodell“ is jól szemlélteti. Az alapfolyamat irányítását, az alarm és kezelői beavatkozásokat és a védelmi rendszert reprezentáló felületen lyukak vannak, mert az alapfolyamat technológiai, és/vagy gépészeti és/vagy irányítástechnikai tervezésekor elkerülte a figyelmet néhány kölcsönhatás és/vagy határérték, vagy, mert a kezelő téveszt és/vagy ignorálja az alarmjelzést, vagy, mert a vész-, védelmi rendszer valamely eleme meghibásodott és/vagy karbantartás állapotban van. E lyukak a különböző környezeti

hatásoknak, meghibásodásoknak, felhasználói viselkedéseknek megfelelően dinamikusan vándorolnak. Mindezek miatt fontos e rendszerek függetlensége és célirányos, adott kockázati szint elérését szem előtt történő tervezése.



3.1. ábra. A baleset kialakulását reprezentáló sajtmodell.

A fenti modell alapján immár látható, hogy a hibákat detektált és nem detektált osztályokba is sorolhatjuk, illetve a hiba bekövetkezte után kialakult állapotokat is kétféle minősítéssel jellemezhetjük:

- Biztonságos állapot: a meghibásodás eredményeképpen a rendszer biztonságos állapotba kerül (spurious trip)
- Veszélyes állapot: a meghibásodás eredményeképpen a rendszer védelmi igény esetén sem tudja ellátni a feladatát.

Jegyzetünkben jelentős hangsúlyt szánunk a kockázatelemzési technikáknak, melyekkel a hiba okok szisztematikus módon feltárhatók, kockázatuk elemezhető.

3.2 Biztonsági integritás –SIL és ASIL értékek

Egy biztonsági rendszer 100%-osan funkcionálisan biztonságos, ha a véletlen meghibásodás, a közös meghibásodás és a szisztematikus meghibásodás nem vezet el a biztonsági rendszer hibás működéséhez, és nem eredményez emberi sérülést, vagy halált, környezetszennyezést, illetve anyagi károkat. Teljes mértékű funkcionális biztonság nem létezik, ugyanakkor az ilyen jellegű események bekövetkezésének várható/megengedhető gyakoriságát az úgynevezett SIL és ASIL értékekkel jellemezhetjük.

Az előző fejezetben említett biztonságkritikus rendszerek kategóriájába való besorolás nem mindig egyértelmű feladat, különösen, hogy most már látjuk, a kockázatcsökkentési akciók után is mindig kell maradandó kockázattal számolnunk. A hibás működés következményei az egyes alkalmazási területeken rendkívül különbözőek lehetnek. A biztonsági integritás (safety integrity – a biztonság sértetlensége) annak valószínűsége, hogy egy biztonsági rendszer az előírt biztonsági funkciókat egy adott időszakban meghatározott körülmények között megfelelően végrehajtja: nem lépett fel

veszélyeztető meghibásodás. Egy rendszerhez rendelt **biztonsági integritási szint (SIL**) meghatározza az alkalmazandó fejlesztési, tervezési, gyártási, üzemeltetési módszereket. Az IEC 61508 és az IEC 61511 szabványok definiálják a biztonság-sérthetetlenség szint (SIL Safety Integrity Level) fogalmát és a szintek meghatározási módszereit. Az IEC 61508 szabvány vezette be a megkülönböztetést az alacsony működtetés igényű és a magas (vagy folytonos) működtetés igényű üzemmód között.

- **Alacsony működtetési igény (Low demand mode):** amikor az adott funkció működtetésének gyakorisága nem nagyobb az egy alkalom/év értéknél, vagy nem nagyobb az úgynevezett proof tesztek gyakoriságának kétszeresénél (Proof teszt: bizonyító erejű teszt. A bizonyító erejű teszt , mely a hibák felderítése céljából végrehajtott periodikus teszt a biztonságosra műszerezett rendszerben, amely mintha új lenne, vagy amennyire praktikusan lehetséges állapotba állítja vissza a rendszert.)
- **Magas, illetve folytonos igény (High demand or continous mode):** amikor az adott funkció működtetésének gyakorisága nagyobb az egy alkalom/év értéknél, illetve nagyobb az úgynevezett proof tesztek gyakoriságának kétszeresénél.

A SIL értéket a termék vagy a kapcsolódó folyamat tervezése során kell rögzíteni, a rendszeres hibák előfordulási gyakoriságának megengedhető értéke alapján. Magasabb SIL érték komolyabb biztonsági követelményeket jelent. A SIL4 a legmagasabb és a SIL1 jelenti a legalacsonyabb követelményt.

3.2. táblázat. SIL értékek alacsony működtetés igényű üzemmód esetén

SIL - Safety integrity level	Alacsony működtetés igényű üzemmód (Az átlagos hibavalószínűség működtetés igényekor)
4	$10^{-5} \leq t < 10^{-4}$
3	$10^{-4} \leq t < 10^{-3}$
2	$10^{-3} \leq t < 10^{-2}$
1	$10^{-2} \leq t < 10^{-1}$

3.3. táblázat. SIL értékek magas vagy folyamatos üzemmód esetén

SIL - Safety integrity level	Magas működtetés igényű vagy folytonos üzemmód (A veszélyes hibák átlagos valószínűsége) Időalap 1 óra.
4	$10^{-9} \leq t < 10^{-8}$
3	$10^{-8} \leq t < 10^{-7}$
2	$10^{-7} \leq t < 10^{-6}$
1	$10^{-6} \leq t < 10^{-5}$

A közlekedésben, energiatermelésben a nem kívánt esemény következménye súlyosságának függvényében a kritikus rendszerekkel szemben általában SIL3 vagy SIL4 követelményeket támasztanak.

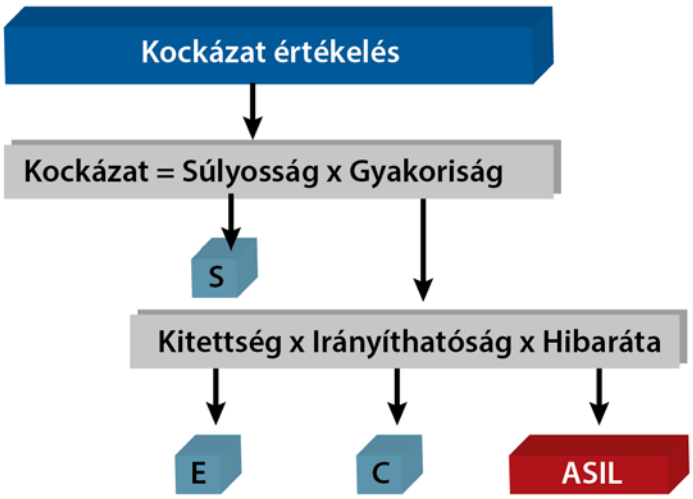
A SIL érték növelése a rendszer célirányos áttervezésével, a kritikus komponensek megbízhatóságának növelésével, illetve – a legkézenfekvőbb módon – redundáns mérő, szabályozó és beavatkozó elemek alkalmazásával érhető el. A redundancia alkalmazhatósága azonban gyakran korlátokba ütközik (költség, méret, súly és rendelkezésre álló energia).

Az elemzés középpontjában a tétel (item), azaz a jármű áll. Az ASIL faktorok becslése a tétel funkcionális viselkedésén alapszik, így a tétel funkcióinak, elvárt viselkedésének részletes leírása szükséges az elemzéshez, szemben a rendszer felépítésével. Ennek szellemében minden szituációt, működési módot le kell írni, mely esetén a tétel hibás működése kockázatot jelent. (pl. normál közúti jármű terepen való közlekedése nagy sebességgel).

A működési szituációkból álló lista összeállítását a tétellel kapcsolatos veszélyhelyzetek szisztematikus gyűjtése követi. Ennek eszközei lehetnek ellenőrzési listák, adatok, meghibásodási statisztikák, FMEA.

A következő lépés a veszélyhelyzetek következményeinek feltárása. Kritikusak azok a hibák, amelyek egyszerre több funkciót is érintenek, illetve sokfajta veszélyhelyzetet okozhatnak (közös-ok hibák, nem független hibák, kaszkád hibák, pl. a tápellátás hibája).

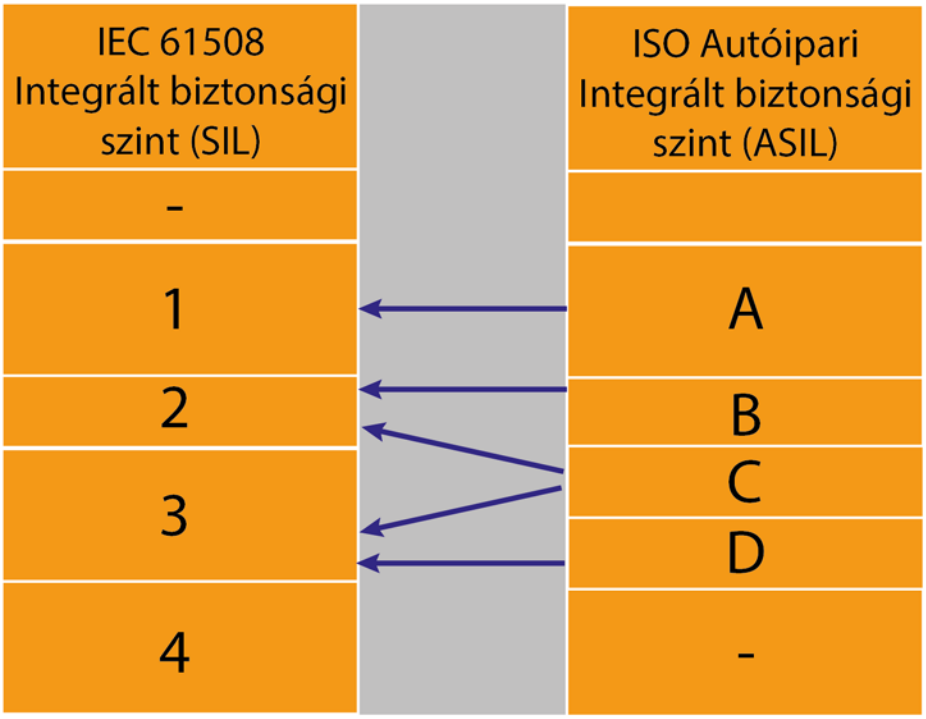
A veszélyes szituációk szisztematikus elemzéséből meghatározhatóak a biztonsági célok és az azokhoz kapcsolódó autóipari biztonsági integritási szintek (ASIL). Az ASIL szintek meghatározásához a következő faktorok hatását kell mérlegelni: súlyosság a baleset bekövetkezése esetén, a kitettség mértéke és szabályozhatóság (irányíthatóság).



3.2. ábra. ASIL érték szerepe a kockázat értékelésben.

Integrált biztonsági szint	Hiba valószínűsége óránként	Legrosszab esetben bekövetkezhet
ASIL A	$< 10^{-6}$	Néhány ember kisebb sérülést szenvedhet
ASIL B	$< 10^{-7}$	Egy vagy néhény ember súlyos, maradó sérülése, vagy egy ember halála
ASIL C	$< 10^{-7}$	Több ember halála
ASIL D	$< 10^{-8}$	Számos ember halála

3.3. ábra. ASIL besorolások



3.4. ábra. Példa ASIL és SIL besorolások megfeleltetésére

Funkcionális biztonságot menedzselni kell, mely a célok számszerűsítésével (az ASIL értékek meghatározását és validálását, illetve a célok elérésének validálását is jelenti).

A funkcionális biztonságot az IEC 61508 szabvány így definiálja: nem megengedhető kockázattól való menteség melyet az E/EP rendszerek hibából eredő viselkedése okoz. E definíció kapcsán fontos, hogy minden hibamódot tesztelni és minden hibát detektálni egy kész rendszer érintő validálás során nem lehetséges, illetve az elemzés a teljes projektet, illetve a termék teljes életciklusát kell, hogy érintse.

4 Megbízhatóság, elérhetőség és biztonság

Az elem megbízhatósági jellemzőinek a segítségével értelmezhetők a rendszer megbízhatósági tulajdonságai. **Megbízhatóság elméleti szempontból rendszer alatt az egymással kapcsolatban lévő elemek egy, a célnak megfelelően körülhatárolt csoportját értjük.** A rendszerek független megbízhatóságú- és nem független megbízhatóságú elemekből épülhetnek fel. Az előbbiek olyan elemekből állnak, amelyeknek a meghibásodása nem vonja maga után a rendszert felépítő többi elem meghibásodását.

A meghibásodások a bekövetkezés ideje szerint lehetnek váratlanok vagy fokozatos mértékben kialakulók. A működőképesség elvesztésének mértéke szerint

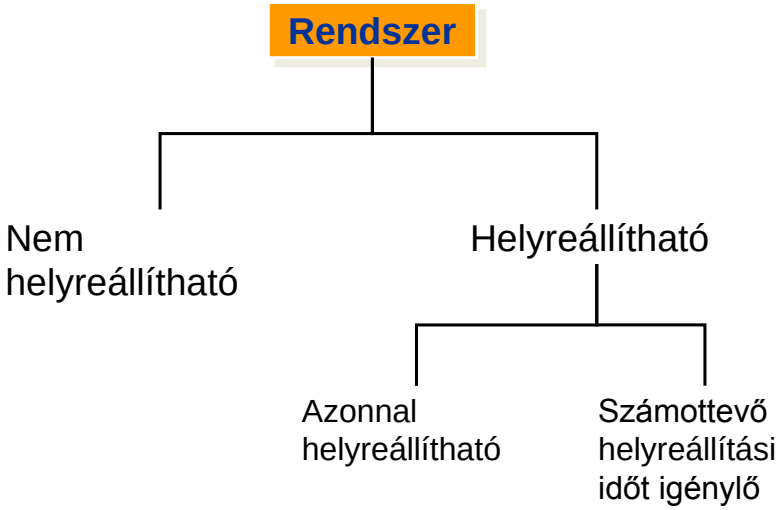
- degradációs
- részleges
- teljes
- katasztrofális

meghibásodásról beszélhetünk.

Az üzembiztos működés szempontjából a legfontosabb kritérium a megbízhatóság (Reliability). Az IEC 61508 szerint a megbízhatóság: „Egy előre megadott idő intervallumban annak valószínűsége, hogy amikor igény van a tervezett művelet végrehajtására, akkor a rendszer végrehajtja azt, feltéve, hogy a rendszer a megadott határértékeken belül működik.”

A rendszer megbízhatóságát, azaz annak a valószínűségét, hogy a kívánt időpontban megfelelő módon funkcionál a rendszer hibamentessége, javíthatósága, tartóssága, tárolhatósága határozza meg.

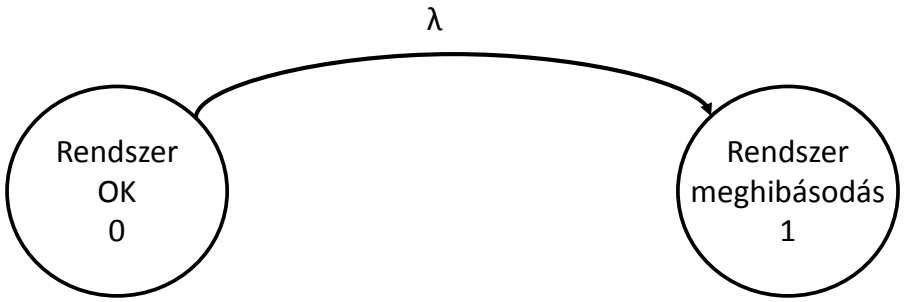
E fejezetben - Dr. Kövesi János (BME) jegyzetére támaszkodva - elsősorban javítható, azaz helyreállítható rendszerekkel foglalkozunk (4.1. ábra).



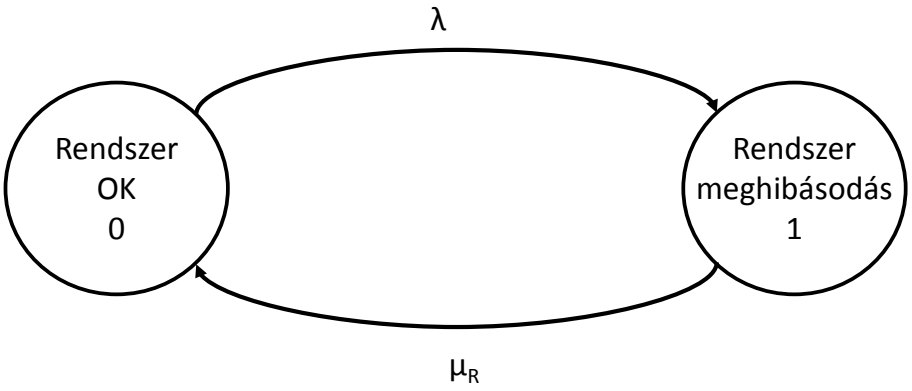
4.1. ábra. Rendszerek osztályozása helyreállósági szempontból.

Tekintettel arra, hogy minden meghibásodásért elvileg véletlenszerűen bekövetkező hibaok a felelős, a meghibásodás bekövetkezésének időpontját nem tudjuk teljes bizonyossággal előre jelezni.

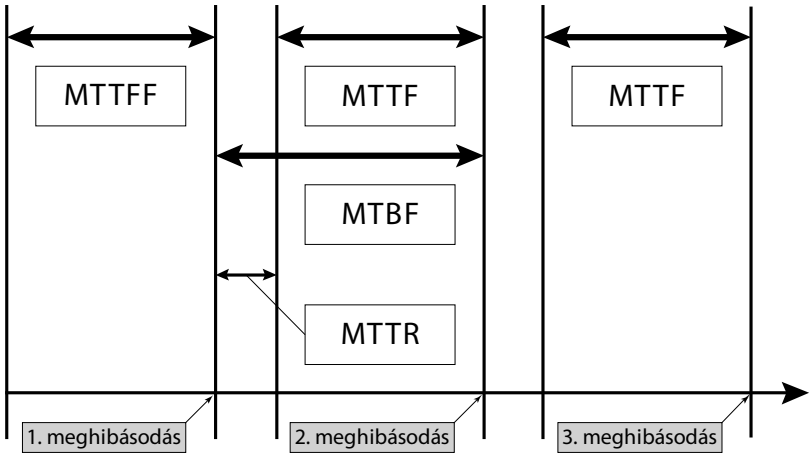
Hasonló módon a helyreállítás szükséges ideje is bizonytalan. Ezért a két meghibásodás közötti hibamentes működési idő és a helyreállítási idő is valószínűségi változó. Egy nem helyreállítható elem meghibásodásáig eltelt hibamentes működési idő, illetve egy helyreállítható elemnél két egymást követő meghibásodás közötti hibamentes működési idő véletlenszerű változó érték (4.4. ábra)



4.2. ábra. Állapotátmenet nem helyreállítható rendszer esetén



4.3. ábra. Állapotátmenetek helyreállítható rendszer esetén



MTTFF (Mean Time To First Failure)
MTTF (Mean Time To Failure)
MFBF (Mean Time Between Failure)
MTTR (Mean Time To Repair)

4.4. ábra. Nevezetes időintervallumok a meghibásodások kapcsán.

Az vázolt meghibásodási és helyreállítási lépésekből álló folyamatnak az egyik alapvető jellemzője a készenléti tényező: **A(t)**, amely annak a valószínűsége, hogy az elem (rendszer) egy tetszőleges t időpontban működik.

$$A = \lim_{t \to \infty} A(t) = \frac{T_1}{T_1 + T_2} \tag{4.1}$$

ahol
T1: MTTF
T2: MTTR

A megbízhatóság nem azonos a rendelkezésre állással. A megbízhatóság t időpontig tartó folyamatos helyességet fejezi ki, a rendelkezésre állás pedig azt, hogy a t időpontban legyen a működés helyes.

A megbízhatóság függvény szabványos jelölése R(t). A megbízhatóság az idő függvényében változik. A megbízhatóság komplement fogalma a hibavalószínűség. A hibavalószínűség függvény az IEC 61508 szerinti jelölése $\mathrm{PF(t)}$. Probability of Failure: Hibavalószínűség. Az IEC 61508, az IEC 61511, az ANSI/ISA 84, stb. a $\mathrm{PF(t)}$ jelölést használja (A magyar szabvány $\mathrm{F(t)}$-vel jelöli.). A két fogalom kapcsolata:

$$\mathrm{PF(t)} = 1 - \mathrm{R(t)} \tag{4.2}$$

4.1 Meghibásodási valószínűségi modellek

A meghibásodási valószínűségi modellek feladata, hogy a funkció rendelkezésre nem állásának időbeli változását definiálják. Egyszerűbb számításoknál a bonyolultabb modellek helyett az időbeli átlagértéket is szokás használni.

Már a megbízhatóság fogalmai is rávilágítanak arra, hogy **a megbízhatóság matematikai modellezése valószínűség számítási és matematikai-statisztikai alapokon** történhet. Feltételezve az alapvető valószínűség számítási ismereteket, a következőben a bizonyítások és a részletes levezetések mellőzésével néhány fontosabb megbízhatóság elméleti összefüggést mutatunk be.

Tekintsünk egy nem helyreállítható, vagyis az első meghibásodásig működő elemet. Jelölje τ valószínűségi változó a hibamentes működési időt, vagyis kezdjen az elem a $t = 0$ időpontban működni és a meghibásodás a $t = \tau$ időpontban következzék be. Ekkor az

$$F(t) = P(\tau < t) \tag{4.3}$$

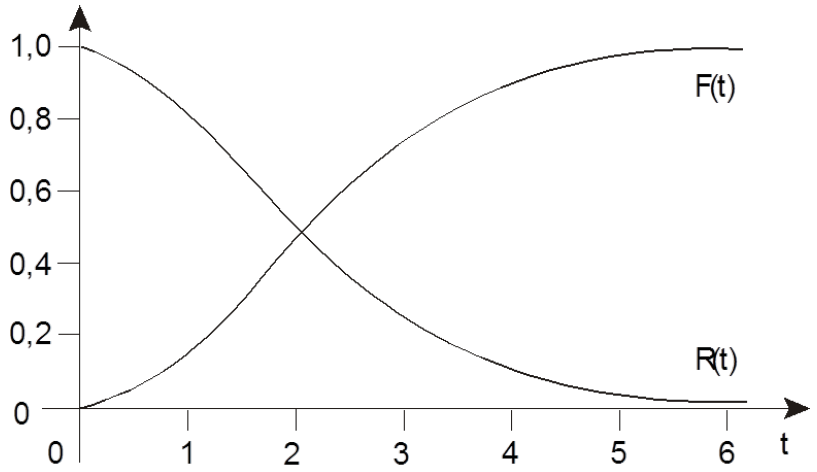
eloszlásfüggvényt a **meghibásodási valószínűség eloszlásfüggvényének** nevezzük, amely tehát a t időpontig bekövetkező meghibásodás valószínűségét fejezi ki. Az F(t) helyett gyakran a hibamentes működés R(t) valószínűségi függvényét, vagy megbízhatósági függvényt használják:

$$R(t) = P(\tau \geq t) = 1 - F(t) \tag{4.4}$$

A τ valószínűségi változónak, mint folytonos valószínűségi változónak van sűrűségfüggvénye, vagyis létezik olyan $f(t) \geq 0$ függvény, hogy a τ valószínűségi változó bármely (a,b) intervallumba esésének valószínűsége megadható az alábbi összefüggéssel:

$$P(a \leq \tau \leq b) = F(b) - F(a) = \int_a^b f(t)dt \tag{4.5}$$

Az eloszlásfüggvény lefutásának jellegét a 4.5. ábra mutatja be.



4.5. ábra. Eloszlásfüggvény, megbízhatósági függvény.

Számos adatbázis (OREDA, FMD, stb.) közli az elektronikus és mechanikus eszközök, berendezések λ meghibásodási rátáját. A λ meghibásodási ráta meghatározásának mérési eljárása alapján is kiszámítható az **átlagos meghibásodási idő**, amit a szabványok MTTF-el (Mean Time To Failure) jelölnek:

A berendezés üzemelés életciklusa alatt a λ meghibásodási ráta állandó. Időben folytonos vizsgálatakor exponenciális eloszlás esetén a berendezés megbízhatóságának időbeli lefolyása az alábbi kifejezéssel adható meg:

$$R(t) = e^{-\lambda t} \tag{4.6}$$

Ugyancsak az (4.2) kifejezés felhasználásával a berendezés hibavalószínűsége:

$$PF(t) = 1 - R(t) = 1 - e^{-\lambda t} \tag{4.7}$$

Az IEC 61508 szabvány vezette be a megkülönböztetést az alacsony működtetés igényű és a magas működtetés igényű[1] üzemmód között.

A magas működtetés igényű berendezéseket a kezelőszemélyzet folyamatosan figyeli és intézkedik. Ilyenkor a veszélyes hibák hibavalószínűségének $PF_D\left[h^{-1}\right]$ átlaga a megbízhatóság mérőszáma.

A PF_{Davg} [2] értékének meghatározása:

$$PF_{Davg} = \frac{1}{T}\int_0^T PF_D(t)\,dt \tag{4.8}$$

Az alacsony működtetés igényű berendezés vagy rendszer hibás állapota akkor derül ki, amikor igény van a működtetésükre. A hibavalószínűség működtetéskor $\left(PF_D\left[year^{-1}\right]\right)$ annak a valószínűsége, hogy az alacsony működtetés igényű rendszer nem működik előírás szerint egy potenciálisan veszélyes helyzetben. Az **átlagos hibavalószínűség működtetéskor** PFD_{avg} [3] az alábbi kifejezéssel adható meg:

$$PFD_{avg} = \frac{1}{TI}\int_0^{TI} PFD(t)\,dt \tag{4.9}$$

ahol a „TI" a bizonyító erejű tesztek[4] közötti időintervallum.

A hibamentesség további jellemzésére **a hibamentes működés átlagos időtartama, vagyis a két meghibásodás közötti átlagos hibamentes működési idő** szolgál, amely a τ valószínűségi változó várható értéke:

---

[1] Low Demand Mode: a működtetési igény gyakorisága nem nagyobb, mint évente 1, illetve nem nagyobb, mint az ellenőrző tesztek közötti idő kétszerese években mérve per év. High Demand Mode: a működtetési igény gyakorisága nagyobb, mint évente 1, illetve folyamatos működtetés, valamint ha a működtetés igény nagyobb, mint az ellenőrző tesztek közötti idő kétszerese években mérve per év.

[2] PF_{Davg} average Probability of dangerous Failure: a veszélyes hibák átlagos hibavalószínűsége

[3] PFD_{avg} average Probability of Failure on Demand: átlagos hibavalószínűség működtetéskor

[4] Proof test: bizonyító erejű teszt. A bizonyító erejű teszt a hibák felderítése céljából végrehajtott periodikus teszt a biztonságosra műszerezett rendszerben, amely mintha új lenne, vagy amennyire praktikusan lehetséges állapotba állítja vissza a rendszert.

$$T_1 = M(\tau) = \int_0^\infty t f(t) dt \tag{4.10}$$

amely figyelembe véve az $f(t)$ és $R(t)$ függvények közötti alábbi összefüggést:

$$f(t) = F'(t) = \left[1 - R(t)\right]' = R'(t) \tag{4.11}$$

parciális integrálás után a következő egyszerűbb formában is felírható:

$$T_1 = \int_0^\infty R(t) dt \tag{4.12}$$

További fontos és közismert megbízhatósági jellemző a $\lambda(t)$ meghibásodási ráta, vagy meghibásodási tényező.

Ennek értelmezéséhez jelentse A azt az eredményt, hogy az elem hibamentesen működik a (t,t + Δt) szakaszban, B pedig azt az eseményt, hogy az elem hibamentesen működött a korábbi (0, t) szakaszban. Ekkor a feltételes valószínűség ismert definíciója alapján:

$$P(A|B) = \frac{P(AB)}{P(B)} \tag{4.13}$$

A (t,t + Δt) szakaszban történő működés valószínűsége, mint a P (A|B) feltételes valószínűség, az alábbi módon számítható ki:

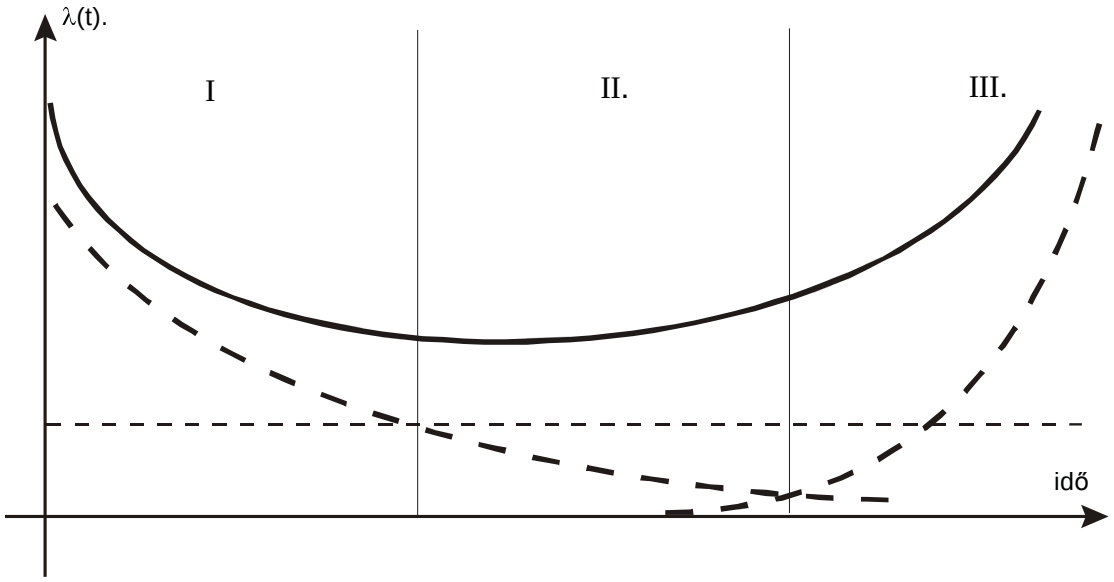
$$P(t, t + \Delta t) = \frac{R(t + \Delta t)}{R(t)} = \frac{1 - F(t + \Delta t)}{R(t)} \tag{4.14}$$

A (t,t + Δt) szakaszban történő meghibásodás valószínűsége pedig, feltéve, hogy az elem a (0, t) szakaszban működött:

$$1 - P(t, t + \Delta t) = \frac{F(t + \Delta t) - F(t)}{R(t)} \tag{4.15}$$

Ha Δt értéke nullához tart, akkor a λ (t) meghibásodási ráta értelmezése a következő összefüggés szerint lehetséges:

$$\lim_{\Delta t \to 0} \frac{F(t + \Delta t)}{\Delta t R(t)} = \frac{f(t)}{R(t)} = \lambda(t) \tag{4.16}$$



4.6. ábra. A „kádgörbe”, azaz a meghibásodási ráta tipikus függvényalakjai

A λ(t) függvény lehet **monoton csökkenő, állandó, vagy monoton növekvő.** Az ábrán látható I-görbe általában olyan elem megbízhatóságát jellemzi, amely még a **„bejáratási szakaszban”** üzemel, így a rejtett hibák gyors felszínre kerülése miatt a λ(t) kezdeti nagy értéke rohamosan lecsökken. A II-görbe a kizárólag **véletlenszerű meghibásodásokkal** jellemezhető üzemeltetési periódusban érvényesül, ahol a meghibásodási ráta közelítőleg állandó mértéken mozog. A III-görbe az **öregedési periódust** írja le, ahol irreverzibilis fizikai-kémiai folyamatok következtében az elem megbízhatósága fokozatosan romlik, vagyis a λ (t) függvény monoton nő. **A λ(t) függvény jellegének pontos ismerete a megbízhatóság alapú karbantartás szervezésben alapvető jelentőségű, így többek között meghatározza az alkalmazható karbantartási stratégia típusát is.**

Az előző ábrán feltüntetett kádgöbe alapján a meghibásodások következő típusai különíthetők el.

I) Korai meghibásodások
- nem megfelelő minőségszabályozás
- nem megfelelő gyártási eljárás
- gyenge minőségű anyagok, kivitel
- rossz felszerelés
- összeszerelési nehézségek
- nem megfelelő hibakeresés
- emberi hibák
- nem megfelelő kezelési módszerek és rossz csomagolás

II) Véletlen meghibásodások
- megmagyarázhatatlan hibaokok
- emberi hibák,
- elkerülhetetlen hibák
- felismerhetetlen hiba
- magas terhelés, igénybevétel

III) Elhasználódás
- nem megfelelő karbantartás

- súrlódás miatti kopás
- öregedés miatti fáradás, kopás
- rossz felülvizsgálati, nagyjavítási gyakorlat
- korrózió

4.2 Megbízhatósági eloszlástípusok

Az előzőekben megismert megbízhatósági jellemzők konkrét értéke természetesen az F(t) eloszlásfüggvény típusától függ. **A megbízhatósági gyakorlatban leggyakrabban alkalmazott eloszlástípusok az exponenciális eloszlás, a Weibull-eloszlás, a normális eloszlás, a lognormális eloszlás és a gamma-eloszlás.** A továbbiakban részletesen csak az első három eloszlástípus jellemzőit mutatjuk be.

Az exponenciális eloszlásfüggvény a következő összefüggéssel írható le:

$$F(t) = 1 - e^{-\lambda t} \qquad (t > 0; \lambda > 0) \tag{4.17}$$

ahol λ az eloszlás állandó paramétere. A meghibásodási ráta definíciója alapján:

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda = állandó \tag{4.18}$$

Belátható az is, hogy az elem átlagos működési ideje:

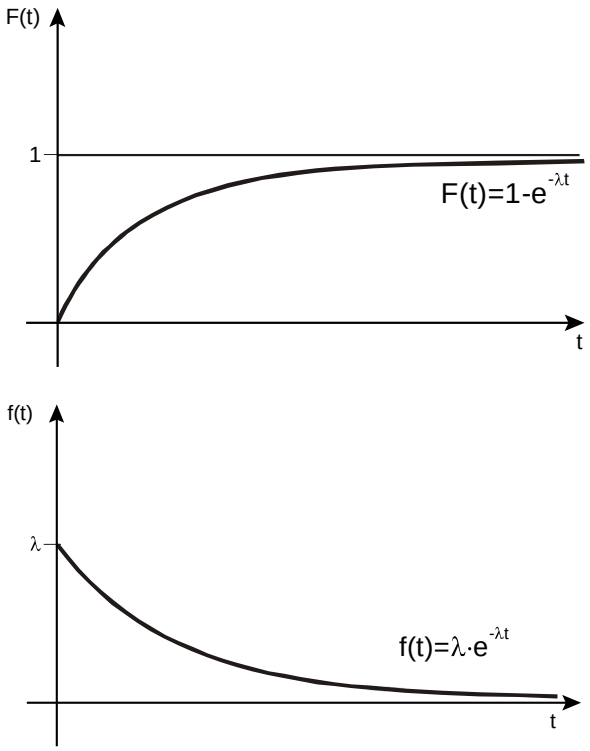
$$T_1 = \frac{1}{\lambda} \tag{4.19}$$

vagyis a meghibásodási ráta az átlagos működési idő reciprok értéke.

A τ valószínűségi változó szórásnégyzete pedig:

$$D^2(\tau) = \frac{1}{\lambda^2} \tag{4.20}$$

A (4.18) összefüggésből következően exponenciális meghibásodási valószínűség eloszlás esetén az elemnek a (t, t + Δt) szakaszban történő meghibásodási valószínűsége független a (0, t) intervallum hosszától. Ez az értelmezése a váratlan jellegű, tehát nem öregedő meghibásodásnak.



4.7. ábra. Exponenciális eloszlás.

Az exponenciális eloszlással jellemezhető rendszerek megbízhatósági függvénye $\mathrm{R}(\mathrm{t}) = \exp(-\lambda t)$.

A megbízhatóságalapú karbantartásszervezés során az egyik leggyakrabban alkalmazott eloszlástípus a Weibull-eloszlás, amelynek F(t) eloszlásfüggvénye a következő:

$$F(t) = 1 - e^{-a.t^b} \; (t > 0; a > 0; b > 0) \tag{4.21}$$

ahol „a” az eloszlás skálaparamétere, „b” pedig az alakparaméter. A meghibásodási ráta:

$$\lambda(t) = \frac{abt^{b-1}e^{-at^b}}{e^{-at^b}} = abt^{b-1} \tag{4.22}$$

tehát egy hatványfüggvény, mely b < 1 esetre monoton csökkenő, b > 1 esetre pedig monoton növekvő. A b = 1 eset megfelel az exponenciális eloszlásnak, így tehát a Weibull-féle eloszlásfüggvény a 6. ábra valamennyi szakaszát leírja.

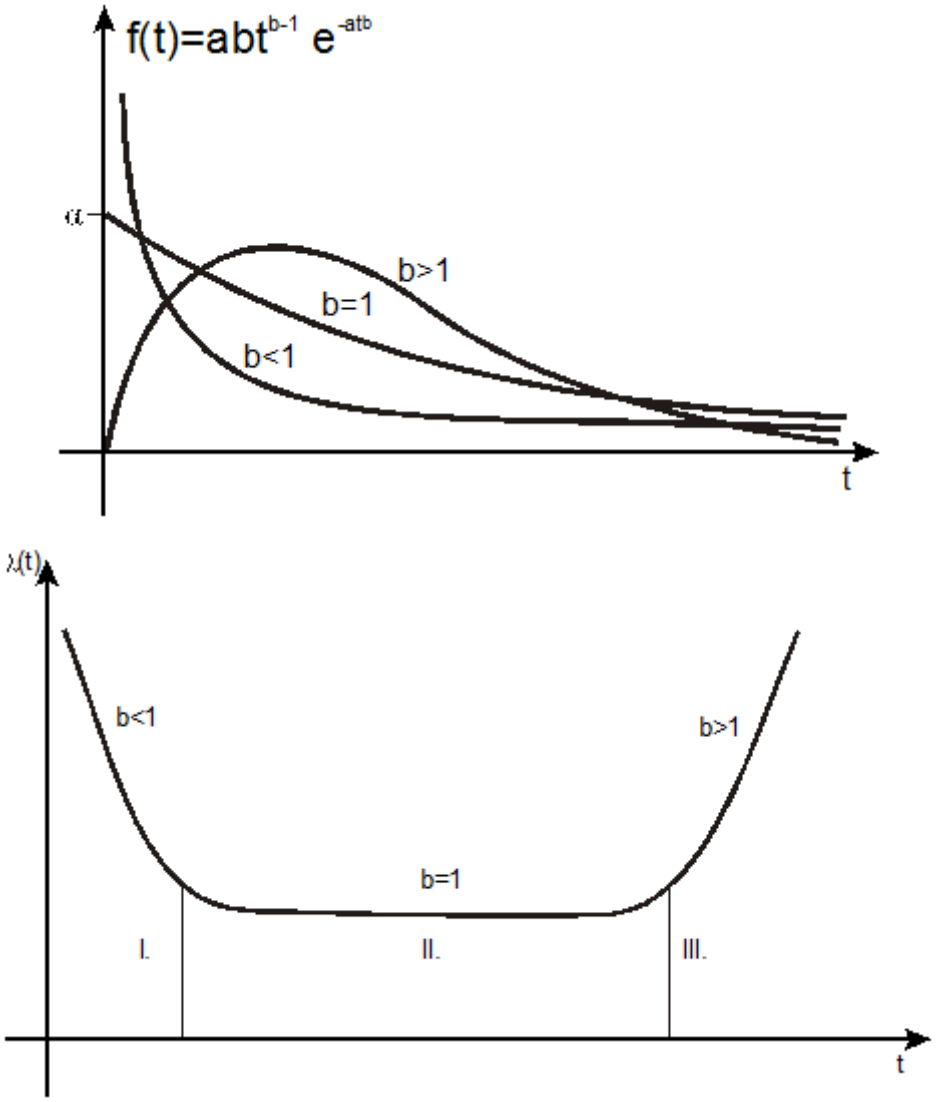
Weibull-eloszlás esetén a τ valószínűségi változó várható értéke és szórásnégyzete az eddigiekhez képest bonyolultabb összefüggésekkel adható meg:

$$T_1 = \frac{\Gamma(1+\frac{1}{b})}{a^{\frac{1}{b}}} \tag{4.23}$$

és

$$D^2(\tau) = \frac{\Gamma(1+\frac{2}{b}) - \Gamma^2(1+\frac{1}{b})}{a^{\frac{2}{b}}} \tag{4.24}$$

ahol „Γ” az Euler-féle gamma-függvényt jelöli, amelynek értékeit a hozzá tartozó táblázat tartalmazza.



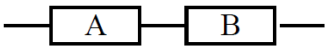
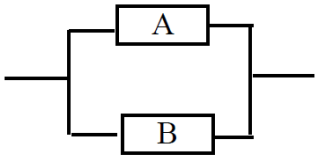
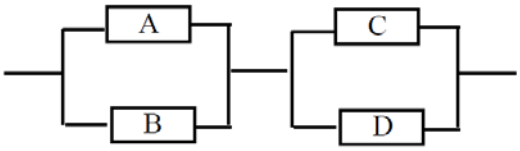
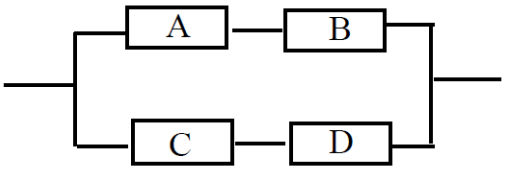
4.8. ábra. Weibull-eloszlás

4.3 Megbízhatósági diagram – összetett rendszerek megbízhatósága

A megbízhatósági blokk diagram egy visszafele haladó (top-down) szimbolikus logikai modell, amelyet a sikerességi tartományban, tehát a helyes működés tartományában definiálunk és generálunk. Minden RBD-nek van egy bemenete és egy kimenete és a modell balról jobbra halad az inputtól az output felé. Az itt megjelenő blokkok egy eseményt, vagy a modellezett rendszer elemeit reprezentálják, azonban általában csupán a rendszere elemeinek függvényét jelentik. Egy rendszerelem lehet akár egy egész részrendszer, egy részegység, komponens vagy bármilyen más része a rendszernek.

Az egyszerű RBD-k soros vagy párhuzamos elemekből, vagy ezek kombinációiból épülnek fel, melyekre az 4.1. táblázat ad példákat. Minden blokk tehát egy eseményt vagy rendszerelem-funkciót reprezentál.

4.1. táblázat. Egyszerű RBD elemek, melyekből egy egyszerű RBD felépíthető. Feltételezzük, hogy az összes elem egymástól függetlenül működik.

Az elem típusa	Block diagram reprezentáció	A rendszer megbízhatósága
Soros		$R_S = R_A * R_B$
Párhuzamos		$R_S = 1-(1-R_A)(1-R_B)$
Soros-párhuzamos		$R_S = (1-(1-R_A)(1-R_B))$ $*(1-(1-R_C)(1-R_D))$
Párhuzamos-soros		$R_S = (1-(1-R_A * R_B))$ $*(1-(R_C * R_D))$

A blokkokat sorosan kötjük össze abban az esetben, ha minden elemnek egyszerre kell helyesen működnie a rendszer helyes működéséhez, míg párhuzamosan, ha bármely elem helyes működése elegendő a teljes rendszer helyes működéséhez. A rendszer nyilván akkor képes üzemelni, ha létezik egybefüggő, folyamatos útvonal a bemenet és a kimenet között.

RBD-vel általában a rendszer megbízhatóságát illusztráljuk, ami nem más mint a helyes működés valószínűsége egy adott időintervallumban. A blokk diagramon minden elemről feltesszük, hogy bármely másiktól függetlenül működik. A kapcsolatot az elemek megbízhatósága és a rendszer megbízhatósága között soros és párhuzamos rendszerek esetén az alábbi képletekkel számoljuk.

Soros rendszer esetén:

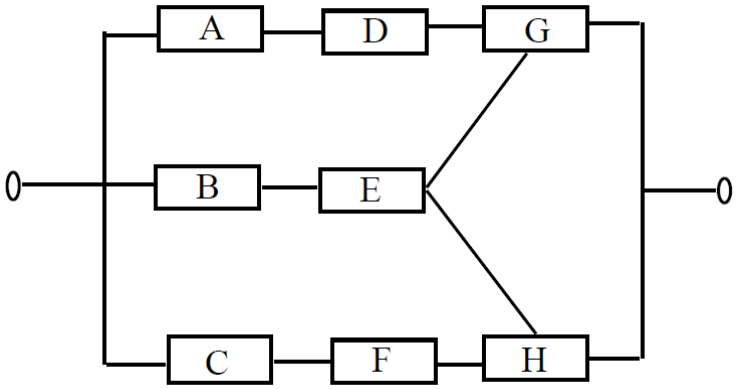
$$R_S = \prod_i^n R_i = R_1 * R_2 * R_3 * \ldots * R_n \tag{4.25}$$

Párhuzamos rendszerre:

$$R_S = 1-\prod_i^n (1-R_i) = \left[1-(1-R_1)*(1-R_2)*(1-R_3)*\ldots(1-R_n)\right] \tag{4.26}$$

ahol R_S a rendszer megbízhatósága, R_i az egyes elemek megbízhatósága, n a rendszerben lévő elemeknek a száma.

Természetesen nem minden rendszert tudunk ilyen egyszerű RBD-kel leírni, a komplex rendszereket nem tudjuk tisztán soros és párhuzamos elágazásokkal modellezni, ezeket bonyolultabb blokk diagramokkal kell kezelnünk. Erre mutat példát az 1. ábra, ahol pl. ha az E jelű elem meghibásodik, akkor a B-E-G és B-E-H útvonalak egyike sem lehet sikeres útvonal, tehát az itt látható elrendezés nem valós párhuzamos megoldás.



4.9. ábra Egy tipikus komplex RBD.

RBD-ket sokszor használják különböző lehetséges tervezési konfigurációk kiértékelésére. Természetesen a szükséges alrendszereket és az egyes elemek megbízhatóságait előre meg kell határozni, különben képtelenek lennénk a rendszer megbízhatóságát kezelni. A technikát általában a projektek tervezési-fejlesztési fázisában alkalmazzák, és előfordul, hogy elemek vagy logikai kapuk azonosítására használják, melyeket aztán a következő fejezetben bemutatásra kerülő hibafákban alkalmaznak.

A fejezetben megnézzük, milyen lépésekből áll egy egyszerű RBD generálása, és egy egyszerű példán is végigmegyünk az elmélet gyakorlati alkalmazásának szemléltetésére.

1) A rendszert részekre, elemeire bontjuk. Hasznos ha rendelkezésre áll egy funkcionális diagram.
2) Az 4.1. táblázatban látható jelölésekkel és elemekből felépítjük a blokk diagramot.
3) Kiszámítjuk a rendszer megbízhatósági tartományát, alsó (R_{SL}) és felső (R_{SH}) határát, valamint minden elemre is kiszámoljuk ezen tartományokat, alsó (R_{iL}) és felső (R_{iH}) határokat, az alábbi képletekkel:
   a. *n* függetlenül működő elemből álló soros rendszer esetén:

$$R_{SL} = \prod_{i}^{n} \left(R_{iL} \right) = R_{1L} * R_{2L} * R_{3L} * \ldots R_{nL} \tag{4.27}$$

$$R_{SH} = \prod_{i}^{n} \left(R_{iH} \right) = R_{1H} * R_{2H} * R_{3H} * \ldots * R_{nH} \tag{4.28}$$

b. n függetlenül működő elemből álló párhuzamos rendszer esetén:

$$R_{SL} = 1 - \prod_{i}^{n} \left(1 - R_{pL}\right) = \left[1 - \left(1 - R_{1L}\right) * \left(1 - R_{2L}\right) * \left(1 - R_{3L}\right) * \ldots * \left(1 - R_{nL}\right)\right] \quad (4.29)$$

$$R_{SH} = 1 - \prod_{i}^{n} \left(1 - R_{pH}\right) = \left[1 - \left(1 - R_{1H}\right) * \left(1 - R_{2H}\right) * \left(1 - R_{3H}\right) * \ldots * \left(1 - R_{nH}\right)\right] \quad (4.30)$$

c. Soros-párhuzamos rendszerek esetén először az egyes párhuzamos ágak megbízhatóságát meghatározzuk a 3.b. pontban leírt képletekkel, majd minden párhuzamos ágat egyetlen elemként kezelve, kiszámoljuk a rendszer megbízhatóságát mint elemek sorba kapcsolt rendszerét a 3.a. pontban lévő képletekkel.

d. Párhuzamos-soros rendszerek esetén, először az egyes soros ágak megbízhatóságát számoljuk ki a 3.a. pontban leírt képletekkel, majd ezen ágakat elemekként kezelve meghatározzuk a rendszer megbízhatóságát, mint elemek párhuzamosan kapcsolt rendszerét a 3.b. pontban ismertetett képletekkel.

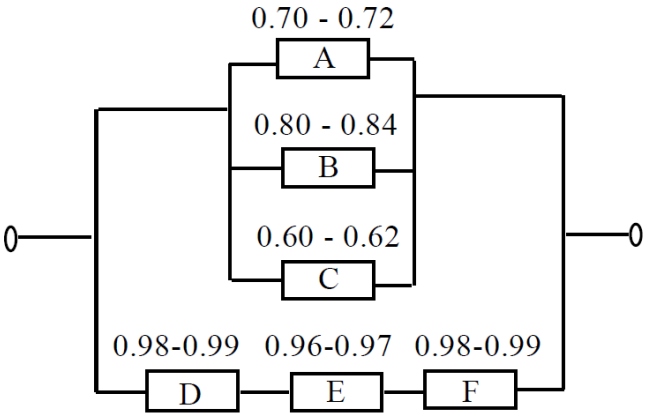
e. Olyan rendszerek esetén, melyek az előző négy elrendezésű részekből épülnek fel, az alábbi módon járunk el. Meghatározzuk a legegyszerűbb ágak megbízhatóságát, majd ezeket elemekként kezelve a megmaradt ágakban ismét kiértékeljük a legegyszerűbb ágakat. Ezt a folyamatot addig folytatjuk, míg már a fenti elrendezések közül csak egyetlen struktúra marad, és azt kiértékelve megkapjuk a rendszer megbízhatóságát.

Nézzünk egy olyan példát, melyben a rendszer két alrendszerből áll, jelölje ezeket S_1 és S_2. S_2-t arra tervezték, hogy az egyes rendszer biztonsági mentéseként funkcionáljon. S_1-ben 3 komponens található, melyek közül legalább egynek működnie kell ahhoz hogy az alrendszer működhessen. S_2-ben ugyancsak 3 komponens dolgozik, melyeknek azonban mindnek egyszerre kell működnie az alrendszer működéséhez. A rendszerben lévő komponensek 10 éves historikus adatokból meghatározott sávjait az alábbi táblázat mutatja.

4.2. táblázat. A példában szereplő komponensek megbízhatósági sávja historikus adatokból.

Alrendszer	Komponens	Megbízhatósági tartományok	
		Alsó	Felső
S_1	A	0.70	0.72
S_1	B	0.80	0.84
S_1	C	0.60	0.62
S_2	D	0.98	0.99
S_2	E	0.96	0.97
S_2	F	0.98	0.99

A rendszerhez felrajzolható RBD-t mutatja a 4.2. táblázat. Amint látható, S_1 komponensei párhuzamos ágakon helyezkednek el a második alrendszer komponenseivel, és S_1 komponensei az alrendszeren belül is párhuzamosan rendeződnek el.



4.10. ábra. A példában szereplő rendszerhez generált RBD.

Az ismertetett képletekkel számoljuk ki a rendszer megbízhatósági tartományát S_1-re, S_2-re, majd az egész rendszerre.

$$R_{1L} = 1-(1-0.70)(1-0.80)(1-0.60) = 0.976$$

$$R_{1H} = (1-(1-0.72)(1-0.84)(1-0.62) = 0.983$$

$$R_{2L} = (0.98)(0.96)(0.98) = 0.922$$

$$R_{2H} = (0.99)(0.97)(0.99) = 0.951$$

$$R_{SL} = 1-(1-0.976)(1-0.922) = 0.998$$

$$R_{SH} = 1-(1-0.983)(1-0.951) = 0.999$$

Tehát a rendszer megbízhatósági tartomány a [0.998, 0.999] intervallum.

Az RBD tehát egy olyan elemző technika, mellyel képesek vagyunk egy rendszer megbízhatóságának alsó illetve felső korlátait becsülni. A módszer során soros és párhuzamos struktúrák használatával építjük fel a blokk diagramot, meghatározzuk az egyes komponensek megbízhatósági tartományát, majd ezek felhasználásával a bementtől a kimenet felé haladva a megbízhatóságokat származtatva kiszámoljuk a teljes rendszer megbízhatósági tartományát.

Előnyök

1) Lehetővé teszi a tervezési koncepciók korai kiértékelését.
2) Általában könnyebben vizualizálható az analízist végző számára, mint más logikai modellek, pl. a hibafa.
3) Az RBD-ben lévő elemeket tudjuk úgy rendezni, hogy az tükrözze a rendszerben lévő szerepüket, tehát információt szolgáltathat a komponensek tényleges rendszerbeli helyzetéről.
4) Mivel az RBD-t könnyen vizualizálhatjuk, használhatjuk arra, hogy pl. egy hibafa elemzést végezzünk, a blokk diagramot hibafává konvertálva, aminek módját a későbbi fejezetekben fogjuk látni.

A módszer korlátai

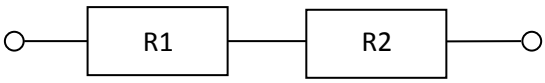
1) Az elemzés során a rendszert részeire kell bontanunk, és meg kell becsülni a részek megbízhatóságát. Az ilyen fajta részekre bontás komplex rendszereknél általában nagyon erőforrás-igényes feladat.
2) A rendszer elemeihez nem mindig állnak rendelkezésünkre megbízhatósági információk. Sokszor ezek becslése nagyon szubjektív, nehezen validálható és esetleg más döntéshozók részére elfogadhatatlan értékeket képviselnek. Komoly problémákat vet fel az is, ha az elemek megbízhatósági értékei más-más konfidencia szinttel rendelkeznek.
3) Nem minden rendszer modellezhető soros, párhuzamos, soros-párhuzamos és párhuzamos-soros elemek kombinációjával. Ezen rendszerekhez komplex RBD-re van szükség, azonban az ilyen RBD-k esetén a megbízhatóságok számolása nagymértékben bonyolódik.

A rendszerek megbízható működésének modellezésére, és ennek felhasználásával a rendszer megbízhatósági jellemzőinek (főként a hibamentességi és használhatósági jellemzőknek) a becslésére számos módszer áll rendelkezésre (pl. hibafa-elemzés, Markov-módszer). Ezek közül a **megbízhatósági diagram** módszerét alkalmazzák leginkább a gyakorlatban. A megbízhatósági diagram a rendszer megbízható működésének grafikus leírására szolgáló eljárás. Megmutatja, hogy milyen logikai kapcsolat van a rendszer működéséhez szükséges működő elemek (alkatrészek) között.

A Megbízhatósági (hibamentességi) folyamatábra (Reliability block diagram) RBD a veszély meghatározására szolgáló folyamatábra kidolgozására irányuló módszer. A folyamatábra a rendszer hibamentes működésének képi ábrázolása; a rendszer megfelelő működéséhez szükséges (funkcionális) rendszerelemek közötti logikai kapcsolatot mutatja be. Az ábrából megállapítható az is, hogy hol vannak kettőzések (tartalékolás). A megbízhatósági folyamatábra alkalmazási köre bizonyos mértékig hasonló a logikai összefüggéseket grafikusan megjelenítő eljárásokéhoz, de leginkább a rendszer megbízhatóságának megállapítására alkalmas. A módszer elsősorban nem-javítható rendszerek esetében és ott alkalmazandók, ahol a meghibásodások bekövetkezésének sorrendje nem számít.

A megbízhatósági diagrammal történő elemzés során, feltételezzük, hogy a rendszer elemeinek (az alkatrészeknek) két állapota van, azaz működőképes állapot vagy hibás. Feltételezzük továbbá, hogy az elemek meghibásodásai egymástól függetlenek, s a hiba bekövetkezése nem változtatja meg más elemek megbízhatósági paramétereit. A megbízhatósági diagram szükségképpen nem egyezik meg azzal az összeköttetési rendszerrel, amellyel a rendszert fizikailag leírjuk (pl. a soros megbízhatósági diagram nem jelent az elektrotechnikai értelemben vett soros kapcsolást).

A továbbiakban csak független megbízhatóságú elemekből álló rendszerekkel foglalkozunk. **Az olyan rendszert, amely akkor és csak akkor működik, ha valamennyi eleme működik, megbízhatósági szempontból soros rendszernek nevezzük.**



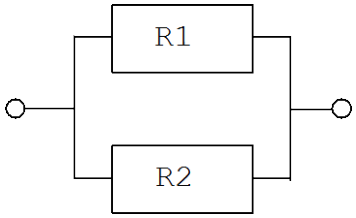
4.11. ábra. Soros rendszer.

Ekkor a rendszer megbízhatósági függvénye:

$$R(t) = \prod_{i=1}^{n} R_i(t) = \prod_{I=1}^{n} \left[1 - F_i(t)\right] \tag{4.31}$$

ahol $R_i(t)$ az i-edik elem megbízhatóság függvényét jelöli.

Az olyan rendszert, amely akkor és csak akkor hibásodik meg, ha valamennyi eleme meghibásodik, megbízhatósági szempontból párhuzamos rendszernek nevezzük:



4.12. ábra. Párhuzamos rendszer.

$$F(t) = \prod_{i=1}^{n} F_i(t) = \prod_{i=1}^{n} \left[1 - R_i(t)\right] \tag{4.32}$$

$$R(t) = 1 - \prod_{i=1}^{n} \left[1 - R_i(t)\right] \tag{4.33}$$

Az összefüggésekből látható, hogy az elemek számának növelésével soros rendszer esetén az eredő megbízhatóság csökken, párhuzamos rendszer esetén pedig nő.

A megbízhatósági függvény értékének ismeretében korábban már általánosan megadtuk a soros ill. párhuzamos rendszerek megbízhatóságának számolását. Behelyettesítve (4.31) és (4.33) összefüggésekbe az R(t) függvényt, megkapjuk az exponenciális működési idővel jellemezhető elemekből felépülő rendszerek eredő megbízhatóságának számolását. Soros rendszerek esetén:

$$R_{soros}(t) = e^{-\lambda_1 t} e^{-\lambda_2 t} \ldots e^{-\lambda_n t} = e^{-(\lambda_1 + \lambda_2 + \ldots + \lambda_n)t} = e^{-\sum_{i=1}^{n} \lambda_i t} \tag{4.34}$$

Soros rendszer esetén tehát, a teljes rendszer működési ideje is exponenciális eloszlású, $\sum_{i=1}^{n}\lambda_i$ paraméterrel. (4.34) képletet felhasználva, a rendszer várható működési idejére ($T_{1,soros}$):

$$T_{1,soros} = \frac{1}{\sum_{i=1}^{n}\lambda_i} \tag{4.35}$$

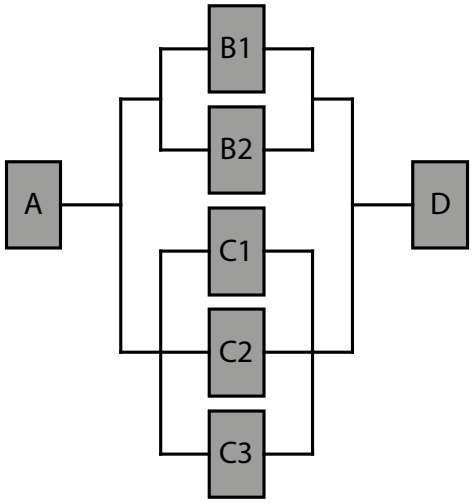
Párhuzamos rendszernél a rendszer működési idő eloszlása már nem exponenciális eloszlással írható le. Behelyettesítve (4.33)-be, s **azonos elemekből** álló rendszert feltételezve, a rendszer megbízhatóságára az alábbi összefüggést kapjuk:

$$R_{párh}(t) = 1-(1-e^{-\lambda t})^n \tag{4.36}$$

ahol λ az azonos elemek konstans megbízhatósági rátája, azaz az eloszlás paramétere. Ekkor a rendszer várható működési ideje:

$$T_{1,párh} = \frac{1}{\lambda}\sum_{i=1}^{n}\frac{1}{i} \tag{4.37}$$

Összetett rendszereket soros, párhuzamos alrendszerekre próbáljuk bontani, s ha ez sikerül, akkor a rendszereredő a fenti képletek alkalmazásával meghatározható.



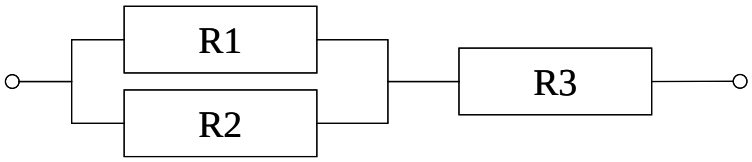
4.13. ábra. Összetett rendszer.

Gyakran előfordul azonban, hogy olyan rendszereket kell modellezni, amelyeket nem tudunk soros-párhuzamos alrendszerekre szétbontani. Ilyen, viszonylag gyakran alkalmazott tartalékolási rendszer például, az ún. n-ből m rendszer is. Ebben az esetben a sikeres működés feltétele az, hogy n számú párhuzamosan kapcsolt elem közül legalább m számúnak kell működnie. Leggyakoribb fajtájuk a 3-ból 2 rendszerek.

Az ilyen, s ehhez hasonló esetekben, amikor is nem lehet a rendszert soros-párhuzamos alrendszerekre szétbontani, segíthet az igazságtáblával történő rendszermegbízhatóság-számolás. Ebben az esetben is feltételezzük, hogy a rendszerelemeknek csak két állapota van, s hogy a megbízhatósági paramétereket a hibák bekövetkezése ill. be nem következése nem befolyásolja. A

módszer lényege, hogy a rendszer minden lehetséges állapotát megvizsgáljuk, kiszámoljuk az állapotok bekövetkezésének valószínűségét. A megbízhatósági diagram segítségével viszonylag egyszerűen meghatározhatjuk az ún. működési utakat, azaz azon állapotokat, amikor a rendszer működik. Ezek állapotvalószínűségeit összegezve megkapjuk a rendszer eredő megbízhatóságát.

Adott az alábbi rendszer, amely akkor működőképes, ha az R3 elem mellett az R1 és R2 közül legalább az egyik működik. Igazságtábla alkalmazásával határozzuk meg a rendszer eredő megbízhatóságát!



4.14. ábra. Összetett rendszer blokkvázlata. R1=0.8; R2=0.9; R3=0.95; Re = 0.931

4.3. táblázat. Lehetséges meghibásodások és hatásaik.

R1	R2	R3	Rendszer-állapot	Állapot-valószínűség	Kumulált működési val.
-	-	-	állás	0,001	
+	-	-	állás	0,004	
-	+	-	állás	0,009	
+	+	-	állás	0,036	
-	-	+	állás	0,019	
+	-	+	működés	0,076	0076
-	+	+	működés	0,171	0,247
+	+	+	működés	0,684	***0,931***

5 Redundáns (szavazó) rendszerek

5.1 Permutáció

A permutációk vizsgálatakor az n-elemű A halmaz elemeit gyakran az első n pozitív egész számmal azonosítjuk. A-nak egy f permutációját úgy adhatunk meg, hogy zárójelben, egymás alá írva, sorbarendezve felsoroljuk az értelmezési tartományát és az értékkészletét. Például $n=5$ esetén az $f(1)=5, f(2)=2, f(3)=1, f(4)=3, f(5)=4$ permutációt a következő rövidebb alakban adhatjuk meg:

$$\begin{pmatrix} 12345 \\ 52134 \end{pmatrix} \tag{5.1}$$

Még rövidebb, ha az elemeknek a séma felső sorában szereplő „természetes sorrendjét" is elhagyjuk, és csak a képelemeket írjuk ki: $(5,2,1,3,4)$.Ez utóbbit néha a permutáció „Descartes-féle alakjának" nevezik.

5.1.1 A permutációk száma

(1,2,3,4)	(2,1,3,4)	(3,1,2,4)	(4,1,2,3)
(1,2,4,3)	(2,1,4,3)	(3,1,4,2)	(4,1,3,2)
(1,3,2,4)	(2,3,1,4)	(3,2,1,4)	(4,2,1,3)
(1,3,4,2)	(2,3,4,1)	(3,2,4,1)	(4,2,3,1)
(1,4,2,3)	(2,4,1,3)	(3,4,1,2)	(4,3,1,2)
(1,4,3,2)	(2,4,3,1)	(3,4,2,1)	(4,3,2,1)

Egy n-elemű halmaz permutációinak számát általában P_n -nel jelöljük. P_n =n!. Ez azért van, mert az 1 képe n különböző érték lehet, ezek minegyikéhez n-1 különböző értéket választhatunk a 2 képéül a fennmaradó számokból, ezek mellé a párok mellé n-2-féleképpen választhatjuk a 3 képét, és így tovább. Az n darab szám képeként tehát n(n-1)(n-2)...1=n!-képpen választhatjuk meg a rendezett értékeket.

A jobb oldali táblázat az {1,2,3,4} számok 4!=24 darab permutációját sorolja fel.

A permutációk számára vonatkozó képlet segítségével több elemi kombinatorikai problémát is megoldhatunk

5.1.2 Az ismétléses permutációk száma

Alkalmanként annak az A halmaznak, amelynek a permutációit vizsgáljuk, bizonyos elemeit megkülönböztethetetlennek tekintjük. Ilyen eset áll elő például, ha egy édességes zacskóban háromféle cukorkából van összesen 30 darab, vagy ha két egyforma csomag kártyát egybekeverünk.

Ha n elem között találunk $k_1, k_2, \ldots, k_m$ egymással megegyezőt, akkor n elem $k_1, k_2, \ldots, k_m$ -ed rendű ismétléses permutációjának nevezzük. Ezeknek számára a $P_n^{(k_1,k_2,\ldots,k_m)}$ szimbólumot szokás használni.

$P_n^{k_1,k_2,\ldots,k_m} = \frac{n!}{k_1!k_2!\ldots k_m!}$ Ennek belátásához lássuk el különböző indexszel az ismétlődő elemeket, hogy felhasználhassuk az ismétlés nélküli permutációk számának meghatározására vonatkozó képletet: $P_{k_1} = k_1!, P_{k_2} = k_2!, \ldots, P_{k_m} = k_m!$. Így megkaptuk az olyan permutációk számát, amelyek megegyeznek egymással (hiszen az indexszel ellátott tagok valójában megegyezők), tehát ezen értékek a szorzatával le kell osztanunk a permutációk számát.

Az 1,2,2,3,3 számjegyekből alkotható ötjegyű számok száma például $P_5^{1,2,2} = \frac{5!}{1!2!2!} = \frac{120}{1 \cdot 2 \cdot 2} = 30$.

5.1.3 A binomiális együtthatók

Gyakran merül föl az a kérdés, hogy egy n-elemű halmazból hányféleképpen választható ki k elem. Ezt az n-től és k-tól függő számot az $\binom{n}{k}$ (kiolvasva: n alatt a k) szimbólummal jelöljük. Nevezetes tény, hogy $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.Ezt az alábbiak alapján úgy láthatjuk be, hogy meggondoljuk: itt a kiválasztott k elemet és a ki nem választott $n-k$ elemet egyaránt megkülönböztethetetlennek tekintjük, tehát valójában egyszerűen a $P_n^{k,n-k}$ kiszámítását kell elvégeznünk. Az $\binom{n}{k}$ szimbólumok szerepet játszanak a kéttagú (idegen szóval binom) összegek hatványainak kiszámításában, ezért ezeket hagyományosan binomiális együtthatóknak nevezzük.

5.2 Redundáns rendszerek koncepciója

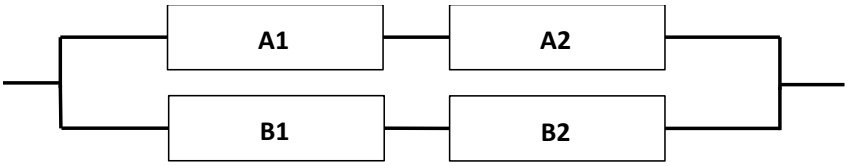
A biztonság kritikus ipari rendszerek esetében a megbízhatóság növelésére az ipari gyakorlatban leginkább redundanciát alkalmaznak, azaz az egyes funkciókat ellátó berendezések megtöbbszörözik. Ha egyszeres redundanciánál összetettebb struktúrát építünk ki, akkor definiálnunk kell azt is hogy a redundáns ágakból minimálisan hánynak kell működnie, másképpen megfogalmazva hány ág meghibásodását tolerálja még a rendszer. Ezek alapján néhány tipikus architektúra a következő:

- 1oo1
- 1oo2
- 1oo3
- 1oo4
- 2oo3
- 2oo4

Kiolvasva az 1oo2: 1 out of 2. Jelentése, hogy a két lehetséges ág közül legalább az egyiknek hibátlannak kell lennie.

5.3 Az 1oo2 rendszer hibakombinációja

Tekintsünk egy 1oo2 architektúrát áganként két elemmel. Az 1oo2 azt jelenti, hogy a két lehetséges ág közül legalább az egyiknek hibátlanul kell működnie.



5.1. ábra. Az 1oo2 rendszer alap struktúrája.

Ebben az esetben az 1oo2 követelmény szerint egy ágnak [$(A1-A2)$ vagy $(B1-B2)$] hibátlannak kell lennie.

A számításhoz a következő értékekre van szükség:

- n A rendszerben lévő elemek száma
- m A hibák száma
- m' A hibás ágak száma

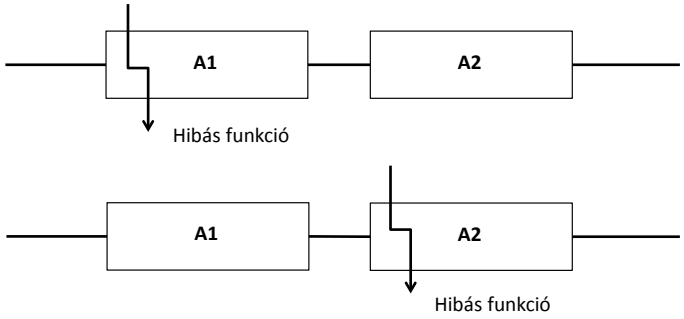
5.3.1 Lehetséges hibák egy ágban

A lehetséges hiba variációk számát először áganként külön tekintsük át. Ha egy ágban csak egy hibát engedünk egy időben, akkor a következő számítás szerint alakul a lehetséges módok száma:

$$\binom{n}{m}=\frac{n!}{n!(n-k)!} \tag{5.2}$$

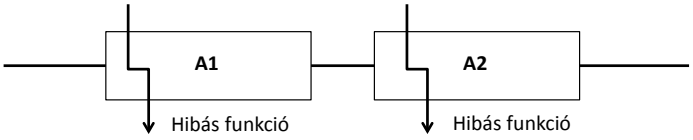
A mi esetünkben pedig:

$$\binom{2}{1}=2$$



5.2. ábra. Lehetséges hibamódok áganként egy hibával.

Ha az ágon belül mindkét elem meghibásodik, akkor kombinatorikailag csak egy lehetséges módozat van.



5.3. ábra. Lehetséges hibamód áganként két hibával.

A kombinatorikai képlet szerint pedig:

$$\binom{2}{2}=1 \tag{5.3}$$

5.3.2 Ágak meghibásodása

Ahogy azt az előbb már láthattuk, egy ágnak három lehetséges meghibásodási módozata van, kettő akkor ha az ágban csak egy hiba van, és egy akkor ha mindkét elem meghibásodik.

Ha több ágat tekintünk egyszerre, és azt engedjük meg, hogy a kettő közül az egyik meghibásodik, azaz $n=2$ ágból a lehetséges hibák száma $m'=1$, akkor a lehetséges variációk száma:

$$\binom{n}{m'}=\binom{2}{1}=2 \tag{5.4}$$

Azaz, vagy az A vagy a B ág, de a kettő együtt nem. A teljes rendszer meghibásodási módozatait a két kombináció szorzata adja:

$$3*2=6$$

Azaz a rendszernek 6 olyan lehetséges meghibásodási állapota van, mely esetén a rendszer funkciója nem veszik el.

A1	A2	B1	B2	
0	0	0	0	Nincs hiba
0	0	0	1	
0	0	1	0	
0	0	1	1	
0	1	0	0	
0	1	0	1	Elfogadhatatlan
0	1	1	0	Elfogadhatatlan
0	1	1	1	Elfogadhatatlan
1	0	0	0	
1	0	0	1	Elfogadhatatlan
1	0	1	0	Elfogadhatatlan
1	0	1	1	Elfogadhatatlan
1	1	0	0	
1	1	0	1	Elfogadhatatlan
1	1	1	0	Elfogadhatatlan
1	1	1	1	Elfogadhatatlan

5.4. ábra. Az 1oo2 rendszer hibamódjai táblázatos formában.

5.4 Hibakombinációk az 1oo3 rendszerek esetében

Az 1oo3 architektúra esetében a működés feltétel, hogy a lehetséges három ágból legalább egy működjön, azaz (A1-A2) vagy (B1-B2) vagy (C1-C2). A további számításokhoz definiáljuk a következő értékeket.

- n A rendszerben lévő elemek száma
- m A hibák száma
- m' A hibás ágak száma

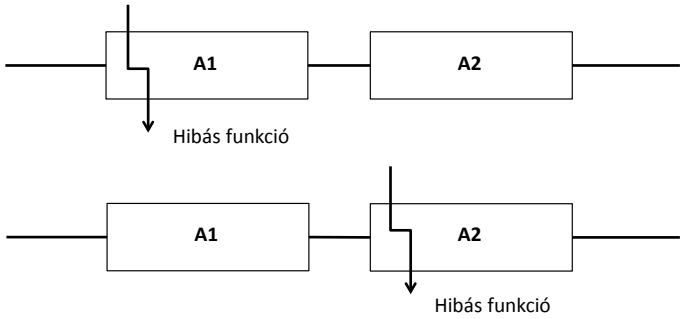
5.4.1 Az 1oo3 rendszer ágon belüli hibamódjai

A lehetséges hiba variációk számát először áganként külön tekintsük át. Ha egy ágban csak egy hibát engedünk egy időben, akkor a következő számítás szerint alakul a lehetséges módok száma:

$$\binom{n}{m} = \frac{n!}{n!(n-k)!}$$

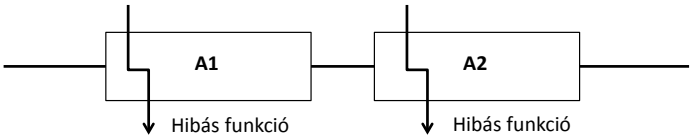
A mi esetünkben pedig:

$$\binom{2}{1} = 2$$



5.5. ábra. Lehetséges hibamódok áganként egy hibával.

Ha az ágon belül mindkét elem meghibásodik, akkor kombinatorikailag csak egy lehetséges módozat van.



5.6. ábra. Lehetséges hibamód áganként két hibával.

$$\binom{2}{2} = 1$$

Az előzőekhez hasonlóan ebben az esetben egy ág három különbözőképpen tud meghibásodni.

5.4.2 Az 1oo3 rendszer egy ág elvesztése

Használjuk a megadott formulát az ágak hibáinak számítására, legyen az $n = 3$, azaz 3 ág van, és a $m' = 1$, azaz egy ág meghibásodását engedjük meg.

$$\binom{3}{1} = 3$$

Azaz három lehetséges módon hibásozhatnak meg az ágak. Az összes lehetséges hibamódot, ahogy a rendszer meghibásodhat az ágon belüli és az ágak közötti hibamódok szorzata adja. A mi esetünkben az ágak 3 módon hibásodhatnak meg, és az ágon belüli elemek is három módon hibásodhatnak meg.

Azaz a lehetséges hibamódok száma: $3 \times 3 = 9$

5.4.3 Az 1oo3 rendszerben két ág elvesztése

A fentiekhez hasonlóan számoljuk ki a meghibásodási módokat akkor, ha két ág is meghibásodik. Ekkor legyen az $n = 3$ és az $m' = 2$. Ekkor az egyenletbe helyettesítve:

$$\binom{3}{2} = 3$$

Két hibás ág esetén az egyes elemek meghibásodása a következő módokon történhet:

- Két elem hibás, mindkét ágban egy-egy.
- Három elem hibás, az egyik hibás ágból mind a kettő, illetve a másik hibás ágból valamelyik.
- Négy hibás elem, mindkét ágból mindkét elem hibás.

5.4.3.1 Két hiba összesen két ágban

Ez a kiépítés úgy állhat elő, hogy mindkét ágban egy-egy elem hibás, ez összes négy lehetőség, mivel:

$$\binom{n_A}{m_A} \cdot \binom{n_B}{m_B} = \binom{2}{1} \cdot \binom{2}{1} = 4$$

Mivel a teljes rendszer három ágból áll, és abból két hibásak háromféleképp tudunk kiválasztani, azaz az ilyen felépítésből is összesen 3 lehetséges. Így a két hibás elemből álló két hibás ágat produkáló meghibásodásból összesen $3 \times 4 = 12$ lehetséges kombináció van.

5.4.3.2 Három hiba két ágban

A fentiekhez hasonlóan számolhat ó ez az eset is, csak itt mindhárom hibának egy ágban kell bekövetkeznie.

A képletbe beírva $n = 2$ és $m = 2$, az eredmény a következő:

$$\binom{2}{1}_a \cdot \binom{2}{2}_b \cdot \binom{2}{1}_c = 2 \cdot 1 \cdot 2 = 4$$

Ebben az esetben az egyes tagok jelentése a következő:

- a Ágak száma két hibával
- b Hibák száma két hiba esetén egy ágban
- c Egyszeres hiba száma egy ágban

Mivel a rendszer most is három ágat tartalmaz, és abból kettőt háromféleképp lehet kiválasztani, így a lehetséges kombinációk száma ebben az esetben is $1 \times 3 = 3$.

5.5 Az 1oo3 esetében a lehetséges hibakombinációk száma

Az előző kombinációk számának összegeként kapjuk meg azoknak a kombinációknak a számát, amikor a teljes rendszer még működőképes marad, azaz

$$9 + 12 + 12 + 3 = 36$$

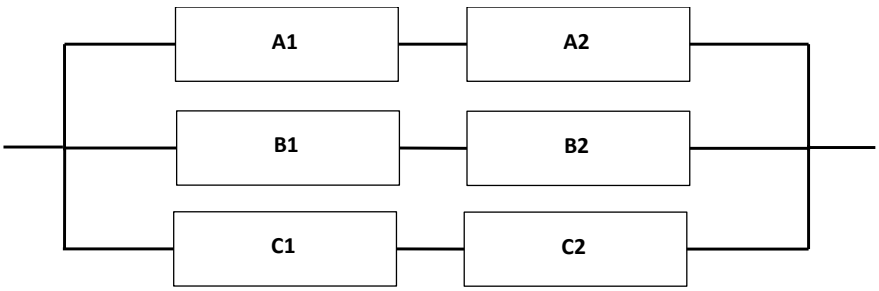
A1	A2	B1	B2	C1	C2		A1	A2	B1	B2	C1	C2	
0	0	0	0	0	0	Nincs hiba	1	0	0	0	0	0	
0	0	0	0	0	1		1	0	0	0	0	1	
0	0	0	0	1	0		1	0	0	0	1	0	
0	0	0	0	1	1		1	0	0	0	1	1	
0	0	0	1	0	0		1	0	0	1	0	0	
0	0	0	1	0	1		1	0	0	1	0	1	Elfogadhatatlan
0	0	0	1	1	0		1	0	0	1	1	0	Elfogadhatatlan
0	0	0	1	1	1		1	0	0	1	1	1	Elfogadhatatlan
0	0	1	0	0	0		1	0	1	0	0	0	
0	0	1	0	0	1		1	0	1	0	0	1	Elfogadhatatlan
0	0	1	0	1	0		1	0	1	0	1	0	Elfogadhatatlan
0	0	1	0	1	1		1	0	1	0	1	1	Elfogadhatatlan
0	0	1	1	0	0		1	0	1	1	0	0	
0	0	1	1	0	1		1	0	1	1	0	1	Elfogadhatatlan
0	0	1	1	1	0		1	0	1	1	1	0	Elfogadhatatlan
0	0	1	1	1	1		1	0	1	1	1	1	Elfogadhatatlan
0	1	0	0	0	0		1	1	0	0	0	0	
0	1	0	0	0	1		1	1	0	0	0	1	
0	1	0	0	1	0		1	1	0	0	1	0	
0	1	0	0	1	1		1	1	0	0	1	1	
0	1	0	1	0	0		1	1	0	1	0	0	
0	1	0	1	0	1	Elfogadhatatlan	1	1	0	1	0	1	Elfogadhatatlan
0	1	0	1	1	0	Elfogadhatatlan	1	1	0	1	1	0	Elfogadhatatlan
0	1	0	1	1	1	Elfogadhatatlan	1	1	0	1	1	1	Elfogadhatatlan
0	1	1	0	0	0		1	1	1	0	0	0	
0	1	1	0	0	1	Elfogadhatatlan	1	1	1	0	0	1	Elfogadhatatlan
0	1	1	0	1	0	Elfogadhatatlan	1	1	1	0	1	0	Elfogadhatatlan
0	1	1	0	1	1	Elfogadhatatlan	1	1	1	0	1	1	Elfogadhatatlan
0	1	1	1	0	0		1	1	1	1	0	0	
0	1	1	1	0	1	Elfogadhatatlan	1	1	1	1	0	1	Elfogadhatatlan
0	1	1	1	1	0	Elfogadhatatlan	1	1	1	1	1	0	Elfogadhatatlan
0	1	1	1	1	1	Elfogadhatatlan	1	1	1	1	1	1	Elfogadhatatlan

5.7. ábra. Az 1oo3 hibakombináció táblázatosan.

5.6 A 2oo3 rendszer hibakombinációi

A fentiekhez hasonlóan szerkesszük meg a 2oo3 rendszer hibamódjait. A rendszer lényege, hogy a három lehetséges ág közül kettőnek mindenképp működnie kell. A számításhoz vegyük alapul a következő változókat:

- n A rendszerben lévő elemek száma
- m A hibák száma
- m' A hibás ágak száma



5.8. ábra. Redundáns rendszer három ággal, áganként két elemmel.

5.6.1 Ágon belüli hibák

Egy ág három különböző módon hibásodhat meg, mivel vagy egy vagy mindkét elem meghibásodik azaz, a lehetséges kombinációk száma:

$$\binom{2}{1}+\binom{2}{2}=2+1=3$$

Ez abból következik, hogy a kettőből egy elem kétféleképpen, mindkét elem pedig egyféleképpen tud meghibásodni.

Ha a három lehetséges ágból egy hibásak háromféleképp tudunk kiválasztani, azaz

$$\binom{n}{m'} = \binom{3}{1} = 3$$

Az összes lehetséges hiba pedig a kettő kombináció szorzatakét adódik, azaz $3 \times 3 = 9$.

5.7 Feladat – Elfogadható hiba redundáns rendszerekben

A redundáns rendszerek lényegében egy elemből tartalmaznak több darabot, így a rendszer az elemek számtól függően képes bizonyos számú elemek tönkremenetele esetén is megfelelően működni. Egy rendszerre megfogalmazott követelmény jelölése:

$$XooY$$

Ahol Y az összes csatorna száma, míg X a mindenképp működőképes csatornák szám. Ha X-nél kevesebb számú csatorna működik megfelelően, akkor a kapott eredmény/adat hibás, azaz nem elfogadható hiba történt. Ellenkező esetben vagy elfogadható hiba történt, csak néhány csatorna került használaton kívülre, vagy mindegyik hibátlanul működik. Minél szigorúbb a feltétel, azaz X minél közelebb van az Y-hoz, annál kevesebb elfogadható hiba van.

5.8 Path Analyzis

Egy módja az elfogadható hibák meghatározásának.

↓ Az algoritmus két egymásba ágyazott ciklusa ↓

```
for i = 1 : max_wrong_channel
    for j = 1 : element
        Fault(i) = Fault(i) + C(element,j);
    end;
    Fault(i) = Fault(i)^i;
    Fault(i) = Fault(i) * C(channel,i);
end;
```

```
function Value = C(n,k)
    if k < n - k
        k = n - k;
    end;
    Value = 1;
    for i = k+1 : n
        Value = Value * i;
    end;
    if (n-k) ~= 0
        Value = Value / (n-k);
    end;
end
```

A külső ciklus először feltételezi, hogy egy csatorna esett ki a rendszerből. Egy csatornán előfordulható hibák száma az ott található elemeke számától függ. Így előfordulhat, hogy egy csatornán egy elem, vagy kettő, vagy az összes elem meghibásodott az egyik csatornán. Ezt számolja a belső ciklus. A „C” függvény lényegében az $\binom{n}{k}$ kombináció értékét számolja ki.

Minden csatornán külön-külön esetként előfordulhat az előző hiba, összesen $\binom{channel}{1}$ féleképpen, így ezzel be van szorozva a „Fault” változó első eleme.

A következő hurok már azt az esetet vizsgálja, amikor 2 csatorna esik ki. Ez már összetettebb eset. Egy csatorna esetére szintén számol a belső ciklus, majd ezt hatványozva, 2 csatornánál 2. hatványra,

n csatornánál n. hatványra emelve megkapható az összes eset. Majd ezt minden csatornára nézve összesen $\binom{channel}{i}$ féleképp fordulhat elő. A táblázatban egyetlen egyféle eset van amikor nincs hiba, amikor minden elem hibátlan, ezért ezek nincsenek kiírva, csupán az összegzett eseteknél (Σ) vehetők észre.

6 Hibafa-elemzés (Fault Tree Analysis - FTA)

A hibafa-elemzés (Fault Tree Analysis – FTA) egy adott balesetre vagy súlyos rendszerhibára (csúcsesemény) összpontosít, és az esemény okainak a meghatározásához ad eljárást. A hibafa olyan gráf, amely a berendezés meghibásodásainak (minimális hibaesemény kombinációk), a nem független meghibásodásoknak és az emberi hibáknak a kérdéses csúcseseményt eredményező különböző kombinációit jeleníti meg. A minimális metszethalmazok meghatározásához a Boole-algebra szabályait alkalmazzák.

Az elemzés során alkalmazott számszerűsítés különbözőképpen történhet, pl. az alapesemény valószínűségének közvetlen becslésével, kinetikus elmélet alapján, Markov-láncok vagy Monte Carlo szimuláció alkalmazásával.

A hibafa-elemzés, mint minőségi elemzési módszer erőssége az, hogy meghatározhatók azok a berendezés-meghibásodási, nem független meghibásodási és emberi hiba kombinációk, amelyek a káros következmény kialakulásához vezethetnek. Ezzel az elemzőnek lehetősége nyílik arra, hogy megelőző intézkedésekkel az alaphibákat célozza meg, és csökkenthesse a bekövetkezési gyakoriságokat. A hibafa elemzés általánosan alkalmazható bármilyen rendszer esetében.

Az analízis egyik első bemutatását Clemens adta 1993-ban [1]. A problémával kapcsolatban a következő évben Goldberg és társai komolyabb kutatásokat végezve egy NASA tanulmányban foglalták össze eredményeiket [2]. Jelen dokumentumban a [2]–ben ismertetett metódust követve ismertetjük a hibafa-elemzési technikákat.

A hibafa-elemzés tehát egy fentről lefele építkező (top-down) szimbolikus logikai modell, melyet a hibatartományon definiálunk és generálunk. Ezzel a technikával képesek vagyunk a csúcseseménytől vagy TOP eseménytől az elemi eseményekig visszakövetni a meghibásodás útvonalát, és meg tudjuk határozni a gyakori meghibásodást okozó elemeket. AZ FTA magába foglalja a hibafa generálását, az elemi események (iniciátorok) meghibásodási valószínűségeinek meghatározását, ezen valószínűségek propagálását a csúcsesemény meghibásodási valószínűségének meghatározására, valamint az ún. cut és path halmazok meghatározását. A tanulmányban mindegyik feladat megoldását végigvesszük.

A tanulmányban ismertetünk 4 elemzési technikát melyeket a komoly baleseti kockázattal járó eseményeket, tevékenységeket tartalmazó rendszerekben meghibásodási valószínűségek becslésére használhatunk. Legnagyobb hangsúlyt a hibafa elemzésre fektetünk, lévén hogy az a legszélesebb körben alkalmazott, és legkiforrottabb technika. Az egyes módszerek egymásba transzformálhatóságára is kitérünk az utolsó fejezetben.

A hibafaanalízis a tervező vagy ellenőrzést végző számára számos, különböző típusú eredményt szolgáltat. Ezek közül egyesek elsősorban a tervezést, a rendszer gyenge pontjainak feltárását segítik elő, míg mások számszerű eredményt adnak a rendszer paramétereiről.

Az egyik legfontosabb vizsgálat a definiált csúcsesemény bekövetkezési valószínűségének számítására irányul. Az analízis során a valószínűség számítás alapszabályai szerint az egyes elemi események valószínűségéből a definiált kapcsolatokon keresztül képezzük a csúcsesemény bekövetkezési valószínűségét. A számszerű eredmény csak azt mutatja meg, hogy a rendszerünk megfelel-e az

elvárásoknak, azt azonban nem, hogy melyek a rendszer gyenge pontjai. A rendszer gyenge pontjairól a minimális vágatok halmazán keresztül szerezhetünk értékes információkat. Minimális vágatnak az elemi események azon halmazát nevezzük, mely elemi események együttes bekövetkezésekor a csúcsesemény bekövetkezik, de amelyek közül bármelyik esemény be nem következésekor a csúcsesemény sem következik be. A minimális vágatokhoz hozzárendelhetjük a bennük szereplő elemi események bekövetkezési valószínűségének szorzatát. Ekkor a minimális vágatokat érték szerint sorba rendezve megállapíthatjuk, hogy elsősorban melyik elemi események felelősek a csúcsesemény bekövetkezéséért.

A minimális vágatok további elemzésével megállapítható, hogy minimálisan hány hiba szükséges a csúcsesemény bekövetkezéséhez. Ez azért fontos jellemző, mert sok esetben a rendszerekkel szembeni meghibásodási valószínűségi követelményeket kiegészítik azzal, hogy a rendszer legyen legalább egyszeresen hibatűrő, vagyis egy hiba, bármilyen kis valószínűséggel is következne be, ne okozhassa a rendszer hibás reakcióját.

Ahogy a továbbiakban látni fogjuk, a hibafa-elemzés legfontosabb feladata a cut és path halmazok meghatározása. Cut halmaznak az elemi (kiindulási, iniciátor) események azon halmazát nevezzük, amelyek mindegyikének bekövetkezése esetén a csúcsesemény is bekövetkezik (nyilván itt minden esetben meghibásodás következik be, hiszen mint említettük az FTA a meghibásodási tartományon operál). Minimális cut halmaznak azt a cut halmazt nevezzük, amely a lehető legkevesebb elemi eseményt tartalmazza. Ezzel szemben a path halmaz azon elemi események egy csoportját jelöli, melyek közül ha egyik sem következik be, akkor az garantálja, hogy a csúcsesemény sem következik be.

FTA-t különösen olyan rendszerekben alkalmaznak, melyeknél magas a komoly baleseti kockázattal járó események, tevékenységek száma. Ez a technika általánosan használható baleseti események azonosítására, azok rangsorolására, és a potenciális baleseti okok beazonosítására. FTA-t általában a projektek tervezési-fejlesztési fázisában használnak, de néha a gyártás-integráció- teszt-értékelés fázisban is helyet kap.

Hibafa elemzés során tipikusan az alábbi feladatokat végezzük el, melyekre a tanulmány további részében részletesen kitérünk.

- Hibafa generálás
- Meghibásodási valószínűségek meghatározása
- Cut halmazok azonosítása és kiértékelése
- Path halmazok azonosítása

6.1 Hibafa generálás

A hibafa-elemzés első lépése a vizsgált rendszer megismerése. Ahhoz, hogy a hibafát felépítsük, előbb pontosan meg kell ismernünk a rendszer működését és azt, hogy a rendszeren belül az egyes elemek miként hibásodhatnak meg. Amennyiben csak korlátozott mennyiségű információ áll rendelkezésre a vizsgált rendszerről, akkor szükség lehet arra, hogy meghibásodásmód és -hatás elemzéssel feltárjuk az összes lehetséges meghibásodást a rendszeren belül. Bármilyen megbízhatósági számítás megkezdése előtt definiálni kell azt az eseményt, amelynek szempontjából számoljuk a rendelkezésre állást (vagy rendelkezésre nem állást) és a meghibásodási gyakoriságot. Ez

azért fontos, mert egy rendszer többféle funkciót valósíthat meg, és a különböző funkciók szempontjából más-más paraméterekkel rendelkezhet.

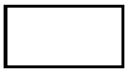
A hibafa-analízisnél a definiált esemény valamilyen hibás működést, vagy a működés elmaradását jelenti. Ezt a definiált eseményt nevezik csúcseseménynek (TOP event). Analízisünk során keressük azokat az ún. elemi eseményeket (Basic event), melyek bekövetkezésekor (esetleg más elemi események bekövetkezésétől függően) a csúcsesemény bekövetkezik. Elemi eseményen olyan eseményeket értünk, melyek bekövetkezési valószínűségéről valamilyen információval rendelkezünk. Fontos az elemi események kapcsolatának helyes felírása, mert ez alapjaiban befolyásolja a számítások eredményét.

A hibafa könnyebb felépítése érdekében definiálhatunk közbenső eseményeket (Intermediate event) is. A közbenső esemény olyan esemény, amely bekövetkezési valószínűsége nem áll rendelkezésre, azt elemi eseményekből számoljuk ki, de ezen közbenső esemény a csúcsesemény szempontjából az elemi eseményekkel azonos módon kezelendő. Közbenső események definiálásával hierarchikus hibafa-rendszert alakíthatunk ki.

A hibafa felépítésekor az események okait az adott rendszer folyamatábráján visszafelé, az eseménytől az ok irányába haladva nyomozzuk ki (deduktív analízis). Minden egyes lépésben veszünk egy okozatot, és keresünk hozzá egy vagy több eseményt (kiváltó okot), amely lehet elemi esemény, vagy közbenső esemény, amelyet a későbbiekben tovább bontunk. (Megjegyzendő, hogy már a hibafa felépítése is igen hasznos segítséget nyújthat: rákényszeríti és rávezeti az analízist végzőt, hogy vegye számba az összes eseményt, amelyek a csúcseseményhez vezethetnek.)

Az események (elemi és közbenső események) között logikai kapcsolatokat definiálunk ún. logikai kapukkal, melyek az összekapcsolt események együttes hatását definiálják a feljebb szinten álló esemény részére. A legtöbb hibafa felépíthető 4 szimbólum segítségével, ami a 2 alap logikai kaput az ÉS-t, és a VAGY-ot, valamint csúcs-, vagy közbenső eseményt és elemi eseményt reprezentáló szimbólumokat foglalja magában. A használható szimbólumok teljes listáját az 1. táblázat tartalmazza.

6.1. táblázat. Hibafa felépítéséhez használható szimbólumok és azok leírása.

	Esemény (csúcs-, vagy közbenső)	Csúcsesemény: a hibás működést, vagy a működés elmaradását reprezentáló esemény, melynek bekövetkezési valószínűségét az analízis során az alsóbb szinten lévő elemek együttes hatásából számoljuk ki. Közbenső esemény: olyan esemény, amely bekövetkezési valószínűsége nem áll rendelkezésre, azt elemi eseményekből számoljuk ki
	VAGY kapu	Az események közül bármelyik bekövetkezése elégséges a következő szint eseményének (esetleg a csúcseseménynek) a bekövetkezéséhez.
	Kizáró VAGY kapu	Csak abban az esetben következik be a következő szint eseménye, ha a bemeneti események közül pontosan egy következett be.
	Kölcsönösen kizáró VAGY kapu	Akkor ad kimenetet, ha egy vagy több, előre meghatározott esemény bekövetkezik, és a többi esemény nem.

	ÉS kapu	Az események együttes bekövetkezése szükséges a következő szint eseményének (esetleg a csúcseseménynek) a bekövetkezéséhez.
	Prioritásos ÉS kapu	Az összes bemeneti esemény adott sorrendben történő együttes bekövetkezése szükséges a következő szint eseményének a bekövetkezéséhez.
	TILTÓ kapu	A feljebb szinten lévő esemény csak akkor következik be, ha az egyetlen bemeneti eseménye bekövetkezik és egy engedélyező feltétel is teljesül.
	Elemi esemény	Olyan esemény, melynek bekövetkezési valószínűségéről valamilyen információval rendelkezünk, így nem szükséges tovább bontatnunk. Levélnek, vagy iniciátornak is nevezik.
	Külső esemény	Olyan külső esemény, mely normál működés esetén várhatóan bekövetkezik.
	Nem meghatározott esemény	Olyan esemény, melyről nem rendelkezünk kellő információval ahhoz hogy további részleteket határozzunk meg róla.
	Feltételes esemény	Feltételek, korlátozások elhelyezésére használjuk, vagy más eseményekhez korlátot rendelhetünk vele.
	NEM kapu	az esemény be nem következése szükséges a következő szint eseményének (esetleg a csúcseseménynek) a bekövetkezéséhez
	K/N	Az N esemény közül legalább K számú bekövetkezése szükséges a következő szint eseményének (esetleg a csúcseseménynek) a bekövetkezéséhez. (Ez a logikai kapcsolat felépíthető ÉS és VAGY kapuk segítségével is, de a K/N logika alkalmazása a kapcsolatrendszert átláthatóbbá teszi.)

Természetesen további logikai kapcsolatok definiálhatóak az előbb felsorolt kapuk segítségével (pl. NAND).

Nem tartozik közvetlenül az események kapcsolatát leíró kapukhoz a transzfer kapu vagy transzfer esemény. A transzfer esemény a hibafa felosztását, lapokra tördelését segíti elő. Egyes közbenső eseményeket (amennyiben azokat transzfer eseményként deklaráljuk), kifejthetünk akár külön rész-hibafában is, elősegítve egyrészt a hibafa érthetőségét, másrészt lehetővé téve azt, hogy egyes közbenső eseményeket több helyre is beillesszünk a hibafába.

A hibafa felépítése olyan folyamat, amely az elemzést végző tapasztaltságától és preferenciáitól függően sokféleképpen végre hajtható. A hibafa felépítése során elkövethető hibák megelőzése érdekében és az elemzést végzők munkájának támogatására több általános szabályt kidolgoztak a kutatók. A szabályok betartásával felépített hibafa helyes és könnyen érthető lesz.

E szabályok lényege a következő:

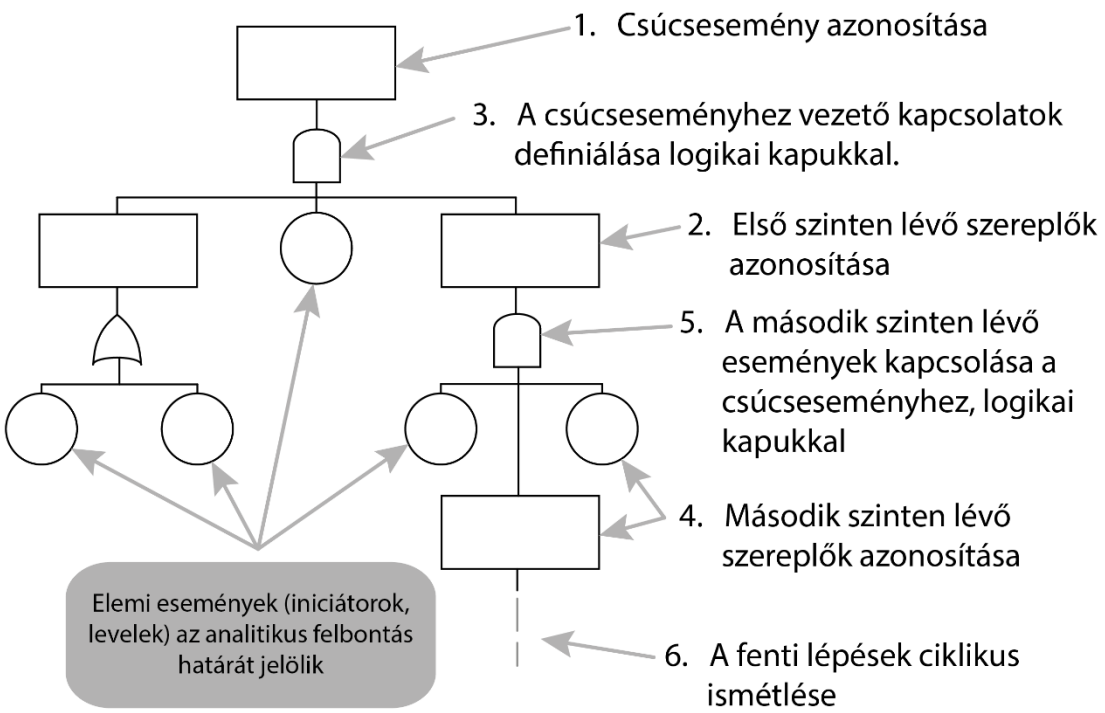
1. **szabály: A csúcsesemény helyes meghatározása:** A hibafa csúcseseményét egyértelműen kell meghatározni és az a rendszernek csak és kizárólag egy üzemmódját és egy meghatározott hibaállapotát jelölje.
2. **szabály: A felépítés iránya: fentről lefelé:** A hibafát mindig fentről lefelé haladva kell felépíteni. A csúcseseménnyel kezdünk, majd az alacsonyabb rendszerszintek felé haladva addig bontjuk tovább a rendszert, amíg elérjük az alapeseményeket.

3. **szabály: A hibaforrás irányába való következetes haladás:** A csúcseseményből kiindulva minden ág kidolgozásakor szigorú következetességgel kell haladni a hibaforrás irányába. Ez mindig igaz, legyen szó akár elektromos, hidraulikus vagy pneumatikus irányítástechnikai folyamatokról. A munka során mindig újabb és újabb irányítástechnikai kapcsolatokra, folyamatokra bukkanunk. Ekkor minden egyes rendszerelem hibát figyelembe kell venni. E szabály betartásával a tévesztés valószínűsége a lehető legkisebbre csökkenthető és a rendszerelemek figyelembe vétele a helyes sorrendben történik meg.
4. **szabály: A kapuk teljes körű meghatározása:** A kapu összes bemenő eseményét teljes körűen fel kell tárni még azelőtt, hogy az események további elemzéséhez hozzáfogunk.
5. **szabály: Nincsenek kapu-kapu kapcsolatok:** A kapu bemenetek mindig pontosan meghatározott hibaesemények, ezért a kapukat más kapukkal közvetlenül összekapcsolni nem szabad.
6. **szabály: Nincsenek csodák:** A rendszer elemzése során esetleg azt találjuk, hogy egy adott hibaesemény-sor hatásának továbbterjedése egy másik rendszerelem valamiféle rendkívüli, teljesen váratlan meghibásodása folytán megszakad. Például nem engedhető meg az a feltételezés, hogy egy szivattyú nyomóvezetékébe beépített visszacsapó szelep „meghibásodás miatt nem nyit”, miután a szivattyú nem megfelelően működött. A helyes feltételezés az, hogy a rendszerelem megfelelően működik, és így lehetővé teszi a vizsgált hibaesemény-sor hatásának továbbterjedését. Ugyanakkor ha egy rendszerelem normális működése egy hibaesemény-sor hatásának továbbterjedését akadályozza, akkor a normális működés helyett szükségképpen meghibásodásoknak kell bekövetkezniük ahhoz, hogy a szóban forgó hibaesemény-sor az adott hibafaágon továbbhaladhasson.
7. **szabály: Az elemzés szükséges részletessége:** Általában kijelenthető, hogy az elemzés részletessége akkor elégséges mértékű, ha az adott eseményhez tartozó meghibásodási adatok rendelkezésre állnak vagy ha az adott esemény bekövetkezési valószínűsége elhanyagolható nagyságú a többi esemény bekövetkezési valószínűségéhez képest.

Néhány javaslat a hibafa felépítéséhez:

1) A fa legyen olyan egyszerű, amennyire a rendszer bonyolultsága ezt egyáltalán lehetővé teszi.
2) Maradjon a fa mindig logikus.
3) Világos, tömör és egyszerű eseményleírásokat válasszunk.
4) A nagy terjedelmű hibafákat bontsuk rész-hibafákra transzferek (átviteli események) segítségével.

A hibafa felépítése tehát egy fentről lefelé haladó elemzési technika, melyet az alábbi ábra szemléltet.



6.1. ábra. A hibafa felépítésének fentről lefelé történő folyamata.

6.1.1 Példa Hibafa generálására

A hibafa-elemzés különböző lépéseit a 6.1. ábra által szemléltetett biztonsági rendszer elemzésén keresztül ismertetjük. A biztonsági rendszer két olyan érzékelőből áll, amelyek megfelelő működéséhez az E2 elektromos betáplálás szükséges. Ha a hőmérséklet a legmagasabb megengedett értéket túllépi a rendszerben, akkor az érzékelők jelet küldenek az egy-a-kettőből funkciójú logikai elemre. Ennek az elemnek külön elektromos tápja (E1) van, és működésekor jelet küld a két azonos beavatkozó elemnek (A1 és A2), amelyek az első forrásból (E2) kapják a tápfeszültséget. A technológiai folyamat leállításához és ezáltal a veszély tényleges létrejöttének megelőzéséhez a beavatkozó elemek egyikének működésbe lépése szükséges.

A példabeli egyes rendszerelemek esetében az alábbi meghibásodási módokat kell figyelembe venni:

Érzékelők : Magas hőmérséklet kialakulásakor nem generál jelet

Logikai elem : Az egyik vagy mindkét érzékelőről érkező jel (jelek) ellenére nem generál működtető jelet a beavatkozó elemek működésbe léptetéséhez

Beavatkozó elemek : Működési igény megjelenésekor nem lépnek működésbe

Feszültségforrás : Nem ad feszültséget a kimeneten

A hibafa felépítése a csúcsesemény meghatározásával kezdődik. A csúcsesemény a hibafa csúcsa, melyet egyértelműen kell meghatározni és az kizárólag a rendszer egy meghatározott üzemállapotára vonatkozhat.

A vizsgált biztonsági rendszer esetében a csúcsesemény a következőképpen definiálható:

„Működési igény fellépésekor a biztonsági védőberendezés meghibásodik”

Ez azt jelenti, hogy ha a hőmérséklet túllépi a legmagasabb megengedhető értéket, akkor a biztonsági rendszer nem állítja le a folyamatot.

Ha a biztonsági rendszer helytelen működésének valószínűségére vagyunk kíváncsiak, akkor a csúcseseményt a következőképpen kell meghatározni:

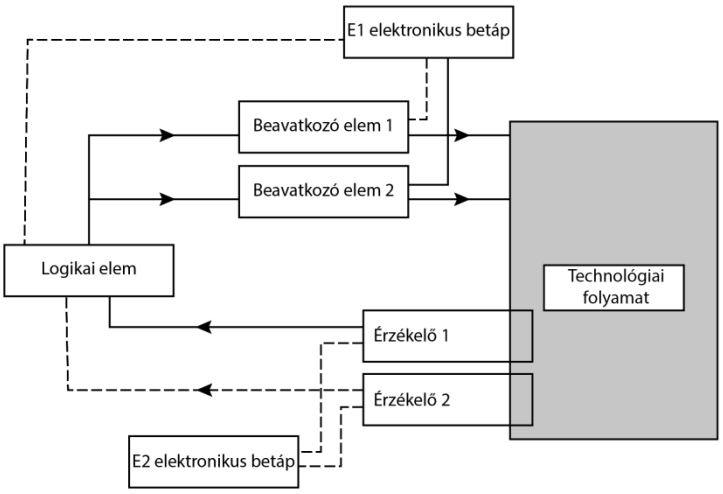
„A biztonsági rendszer helytelenül működik”

Ez azt jelenti, hogy a biztonsági rendszer működési igény megjelenése nélkül („indokolatlanul”) állítja le a folyamatot. A két esetben más és más hibafát kell készíteni.

A csúcsesemény meghatározása után fel kell építeni a hibafát. A hibafa felépítésének célja az, hogy a csúcsesemény bekövetkezéséhez hozzájáruló összes okot feltárjuk. A hibafa elkészítéséhez szükség van a rendszert bemutató rajzok és leírások átvizsgálására. A rendszer felügyeletét, működtetését vagy karbantartását végző személyzet kikérdezésére is gyakran szükség van ahhoz, hogy a csúcseseményhez hozzájáruló összes okot feltárjuk.

Fel kell ismerni, hogy a hibafa a rendszernek csak és kizárólag egy meghibásodási módjára vonatkozik.

A példabeli esetben a biztonsági védőrendszer nem lép működésbe a magas hőmérséklet kialakulásakor.

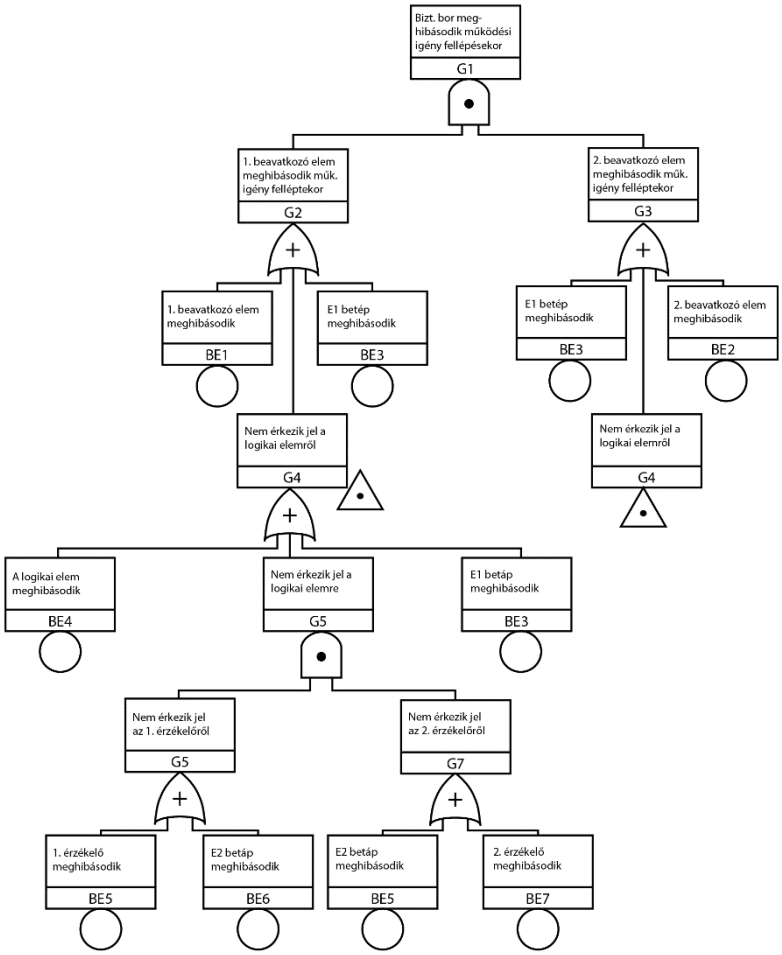


6.2. ábra. A rendszer felépítése

A hibafa képi formában ábrázolja azokat a körülményeket és feltételeket, amelyek kiváltják az előre meghatározott kedvezőtlen esemény bekövetkezését, illetőleg hozzájárulnak ahhoz; e kedvezőtlen eseményt „csúcseseménynek” hívjuk. A vizsgált biztonsági rendszer esetében a csúcseseményt tehát a következőképpen határoztuk meg:

„Működési igény fellépésekor a biztonsági védőberendezés meghibásodik”

A hibafát a 6.3. ábra mutatja.



6.3. ábra. A rendszerre vonatkozó hibafa

A hibafa felépítését a biztonsági rendszer és a folyamat érintkezési pontján kell kezdeni. A példában az 1 és 2 beavatkozó elem állítja le a folyamatot. A hibafa felépítésének tehát ez a kezdőpontja. Figyelembe véve, hogy a két beavatkozó elemből egy szükséges a folyamat leállításához, ezért a folyamat nem áll le, ha egyik beavatkozó elem sem lép működésbe. Ez azt jelenti, hogy „ÉS” logikai kapuval kell kezdeni az összeállítást, mert mindkét beavatkozó elemnek meg kell hibásodnia ahhoz, hogy a csúcsesemény bekövetkezzen.

A G1 kapu bemeneti eseményeként két közbenső esemény határozható meg. Az 1 beavatkozó elem működési igény fellépésekor nem működik és a 2 beavatkozó elem működési igény fellépésekor nem működik.

Ezt követően fel kell tárni mindazokat az okokat, amelyek miatt az 1 elem nem képes működésbe lépni. Ennek során lentről felfelé kell végighaladni azokon a folyamatokon, amelyek az 1 beavatkozó elem megfelelő működéséhez szükségesek.

Háromféle ok miatt fordulhat elő az, hogy az 1 beavatkozó elem a működési igény megjelenésekor nem lép működésbe:

- az 1 beavatkozó elem meghibásodott (belső meghibásodás);
- az E1 nem szolgáltat tápfeszültséget;
- az egy-a-kettőből logikai elem nem ad rendelkező jelet.

E három ok bármelyikének bekövetkezése elégséges ahhoz, hogy a G2-vel jelzett közbenső esemény bekövetkezzen. Ez azt jelenti, hogy a G2 kapu „VAGY" logikai kapu. Ugyanez érvényes G3-ra is.

Három bemenő eseményt kell figyelembe venni G2-höz és G3-hoz is. Két bemenő esemény alapesemény: az egyik a beavatkozó elem belső meghibásodása, a másik az 1 beavatkozó elem elektromos betápjának megszűnése. A harmadik bemenő esemény a G4 kapu kimenő eseménye, amely a rendelkező jelre vonatkozó meghibásodást jelenti.

Hangsúlyozzuk, hogy a G2 és a G3 kapu esetében a különbség abban áll, hogy az első eset az 1 beavatkozó elem belső meghibásodására, a második pedig a 2 elem belső meghibásodására vonatkozik. Az 1 elektromos betáp figyelembevételekor a két kapu esetében nem kell különbséget tenni, mert mindkét esetben ugyanannak a feszültségforrásnak a meghibásodásáról van szó.

A G4 kapuhoz a G2 kapuba való átvitelt jelölő szimbólumot tettünk. Ez arra utal, hogy a G4 kimenetét jelentő ág a G3 bemenő eseményre is érvényes.

Ezután azonosítani kell a működtető jel összes lehetséges meghibásodási okát. A biztonsági rendszer gondos átvizsgálása azt mutatta, hogy három okot lehet megkülönböztetni:

- az egy-a-kettőből logikai elem meghibásodik (belső meghibásodás);
- az 1 feszültségforrás meghibásodik;
- egyik érzékelőtől sem érkezik jel a logikai elemre.

A logikai elem belső meghibásodásának a BE4 alapesemény, az E1 feszültségforrás meghibásodásának pedig a BE3 alapesemény felel meg. A logikai elemek kialakítása miatt (egy-a-kettőből) „ÉS" logikai kapuval kell leírni az érzékelők jeladásra vonatkozó meghibásodását.

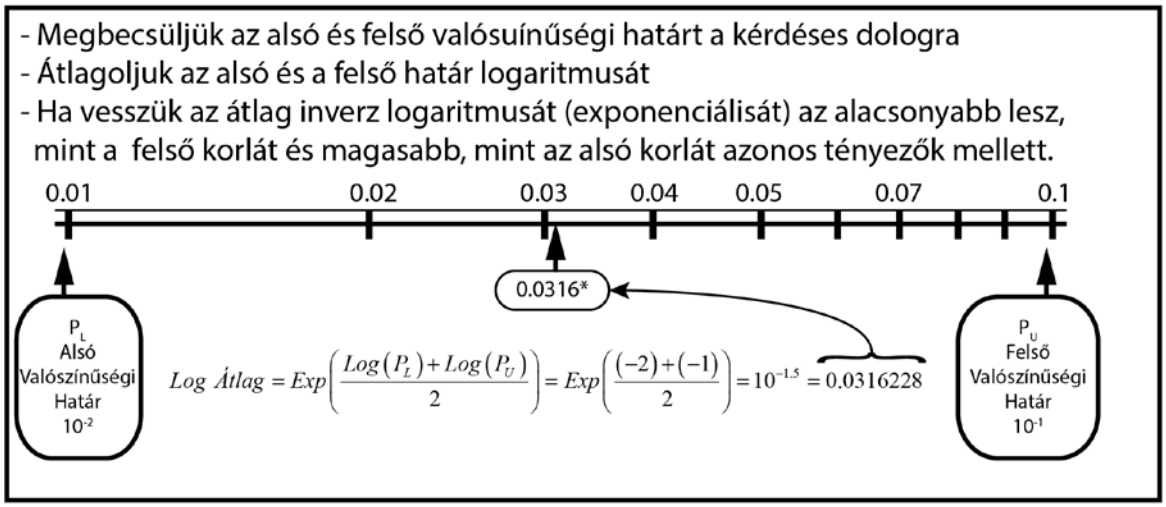
A jeladás folyamatán a forrás felé haladva két különböző okot állapíthatunk meg, amiért az 1 érzékelő nem generál jelet. Az első ok az érzékelő belső meghibásodása, a második pedig az E2 tápfeszültség kiesése lehet. Így tehát azt az eseményt, hogy az 1 érzékelő nem generál jelet, a G6 „VAGY" logikai kapu felvételével kell figyelembe venni. A G6 kapu bemenő eseményei a BE5 alapesemény (az 1 érzékelő meghibásodik) és a BE6 alapesemény (az E2 elektromos betáp meghibásodik). Ezzel analóg módon vezethető le a 2 érzékelő jelküldéssel összefüggő meghibásodása.

6.2 Meghibásodási valószínűségek számítása

Az leggyakrabban alkalmazott logikai kapcsolatokat alapkapcsolatoknak nevezzük, melyek az **ÉS, VAGY, NEM, K/N** kapcsolatok. Ezen kapcsolatok és a csúcseseményt, közbenső eseményeket és elemi eseményeket reprezentáló szimbólumokkal a legtöbb hibafa felépíthető.

A meghibásodás valószínűségek számításának első lépése, hogy meghatározzuk az elemi események bekövetkezésének valószínűségeit. Ez általában valamilyen kvantitatív módszerrel történik, vagy szakértői tudáson alapuló elemzés eredménye. Például, log átlag elemzés használható abban az

esetben, ha a valószínűségeket nem tudjuk becsülni, azonban hihető alsó- és felső korlátokat képesek vagyunk becsülni hozzájuk. Ezt reprezentálja az 6.4. ábra.



6.4. ábra. log átlag elemzés valószínűségek becslésére.

Az elemi események bekövetkezési valószínűségeinek becslése után ezen valószínűségek felhasználásával és a definiált kapcsolatok alkalmazásával a fán felfelé haladva meghatározzuk a köztes események és így végül a csúcsesemény bekövetkezési valószínűségét is. A továbbiakban a leggyakrabban alkalmazott kapcsolatok kimenetének bekövetkezési valószínűségeinek kiszámítási módjait ismertetjük.

Az alábbi példákban rendre P_i jelöli a bemeneti események hibavalószínűségeit, R_i a bemeneti események túlélési valószínűségeit, míg a kimeneti esemény hibavalószínűsége P_T, túlélési valószínűsége R_T lesz.

6.2.1 Alapvető kapcsolatokat megvalósító több bemenetű kapuk kimeneti valószínűsége

Mivel **ÉS** kapcsolat esetén a kimeneti esemény csak abban az esetben következik be, ha minden bemeneti esemény bekövetkezett, így a kimeneti esemény meghibásodási valószínűségét n bemeneti esemény esetén az alábbi képlet adja:

$$P_T = \prod_{i=1}^{n} P_i \tag{6.1}$$

Több bemenetű **VAGY** kapu esetén a kimeneti esemény minden esetben bekövetkezik, ha bármelyik bemeneti esemény bekövetkezett, így a kimeneti esemény meghibásodási valószínűségét n bemenettel az alábbi képlettel számíthatjuk.

$$P_T = 1 - \prod_{i=1}^{n} (1 - P_i) \tag{6.2}$$

A **NEM** kapu egyetlen bemenettel rendelkezik, és mivel a kimenetén lévő esemény pontosan akkor következik be, ha a bemenetén lévő nem, ezért kimeneti valószínűségének képlete:

$$P_T = 1 - P_1 \tag{6.3}$$

Általános M/N kapu esetén az N db bemenet közül legalább M-nek teljesülnie kell a kimeneti esemény bekövetkezéséhez. Így itt a kimeneti valószínűséget az alábbiak szerint számíthatjuk:

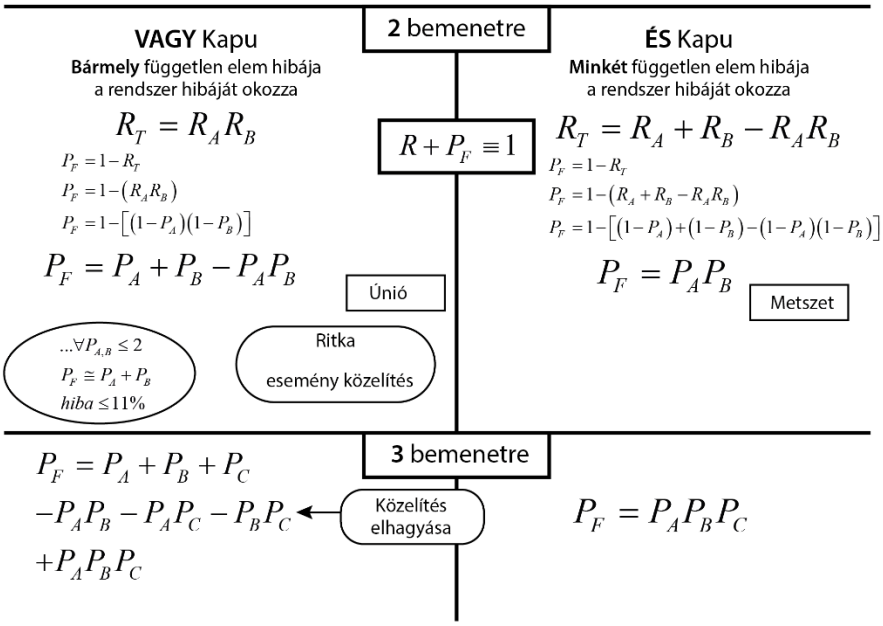
$$P_T = 1 - \prod_{\substack{i_1 \\ i_2 \\ \vdots \\ i_m}} \left(1 - P_{i_1} P_{i_2} \ldots P_{i_m}\right) \tag{6.4}$$

ahol, $i_1 = 1 \ldots (n-m+1) i_1 = i_1 + 1 \ldots (n-m+2), \ldots, i_1 = i_{m-1} + 1 \ldots (n-m+m)$.

vegyünk egy egyszerű 3/4 kaput a fenti képlet alkalmazására. Így a $P_{i_1} \cdot P_{i_2} \cdot \ldots \cdot P_{i_m}$ tag rendre 3 darab P valószínűséget fog tartalmazni. Az i_1 index 1-től $(n-m+1)$-ig, azaz 2-ig fut. Ha $i_1 = 1$, i_2 2 és 3 lehet, ha $i_1 = 2$, i_2 csak 3 lehet. A fenti gondolatmenetet követve számítható i_3 értéke is.

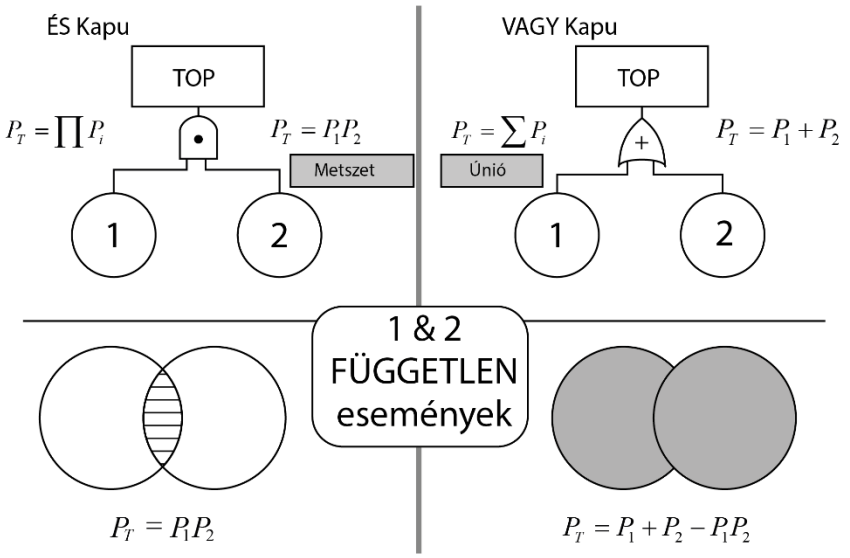
Vagyis

$$P_T = 1 - R_T = 1 - \left[\left(1 - P_1 \cdot P_2 \cdot P_3\right) \cdot \left(1 - P_1 \cdot P_2 \cdot P_4\right) \cdot \left(1 - P_1 \cdot P_3 \cdot P_4\right) \cdot \left(1 - P_2 \cdot P_3 \cdot P_4\right)\right] \tag{6.5}$$



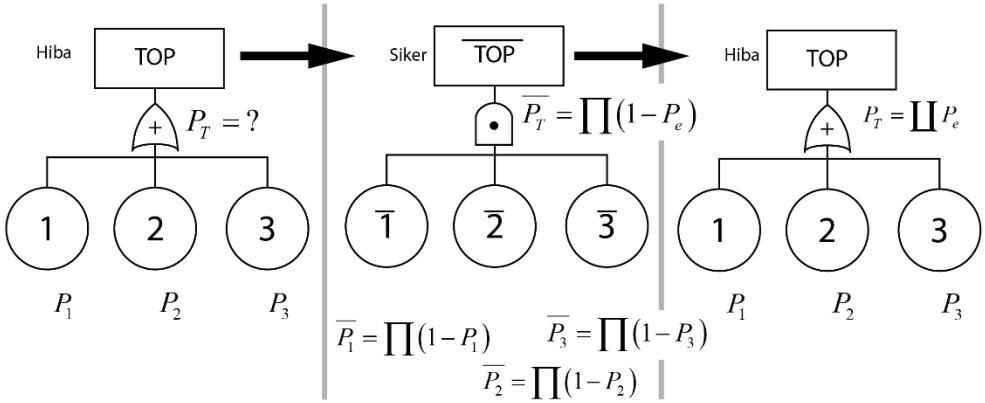
6.5. ábra. 2 illetve 3 bemenetű VAGY illetve ÉS kapu kimeneti valószínűségének számítása.

A kapuk használatának és a segítségükkel a valószínűségek felsőbb szintre történő származtatásának szemléletes magyarázatát adja az alábbi, 6.6. ábra ÉS illetve AND kapuk esetén, 2 bemeneti eseménnyel.



6.6. ábra. Két bemenetű ÉS illetve VAGY kapu kimeneti valószínűségeinek származtatása.

Ahogy a fenti ábrákon is látható, és ahogy korábban is említettük, ezen módszerek a felsőbb szinteken lévő események meghibásodási valószínűségeinek becslését szolgáltatják, még akkor is ha pontosan ismerjük az elemi események valószínűségét. Ez a 6.5 ábrán látható „Rare event approximation" technika alkalmazásából fakad, mely jóval egyszerűbb és gyorsabb számítást tesz lehetővé, csekély információ elvesztése mellett. A gyakorlatban szinte kivétel nélkül ezt a fajta megközelítést alkalmazzák. Viszont természetesen lehetnek olyan speciális esetek, amikor semmilyen közelítést sem engedhetünk meg az analízis során, ekkor az egyes kapcsolatok pontos kiértékelésére van szükség, mely a 6.7 ábrán látható.



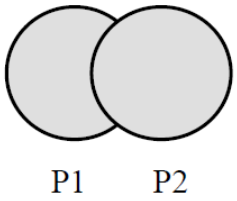
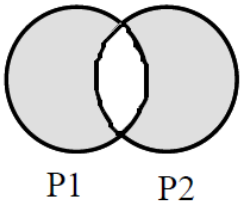
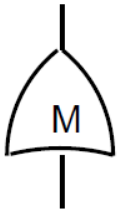
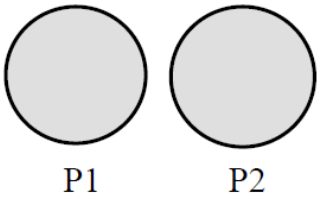
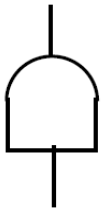
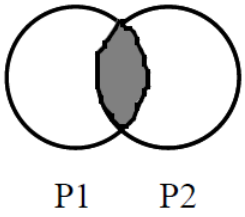
6.7. ábra. 3 bemenetű VAGY kapu pontos kiértékelésének módszere.

Bár nagyon ritkán találkozni a használatával, ilyen esetben speciális operátorokat használnak, így például a n db bemenettel rendelkező VAGY kapu kimeneti valószínűségét az alábbi képlettel számolhatjuk:

$$P_T = \prod_{i=1}^{n} P_i = 1 - P(1 - P_i) = 1 - \left[(1 - P_1)(1 - P_2)\ldots(1 - P_n)\right] \qquad (6.6)$$

A legfontosabb logikai kapuk esetében az ún. terjedési egyenleteket a tartalmazza. Az itt szereplő képletek megadják hogy a bemeneteken jelentkező valószínűségek milyen matematikai számítás szerint haladnak át a kapun, és mi jelenik meg azok kimenetén. A táblázatban a korábban említett elhanyagolásokat is alkalmazva mutatja be a terjedési egyenleteket.

6.2. táblázat. A leggyakrabban használt logikai kapuk esetében a valószínűségek terjedésének képletei

Szimbólum	Név	Venn diagram	Terjedési egyenlet
	VAGY kapu		$P_T = P_1 + P_2 - (P_1 * P_2)$ $P_T = P_1 + P_2$ **
	Kizáró VAGY kapu		$P_T = P_1 + P_2 - (P_1 * P_2)$ $P_T = P_1 + P_2$ **
	Kölcsönösen kizáró VAGY kapu		$P_T = P_1 + P_2$
	ÉS kapu (illetve prioritásos ÉS kapu)		$P_T = P_1 * P_2$

6.3 Minimális vágatok (cut) halmazának meghatározása

Ahogy korábban már említettük, vágatnak vagy cut halmaznak azon események halmazát nevezzük, melyek együttes bekövetkezése esetén a csúcsesemény is bekövetkezik. Ezek közül a legkevesebb eseményt tartalmazót minimális vágatnak nevezzük. Tehát minimális vágatnak az elemi események azon halmazát nevezzük, melyek együttes bekövetkezésekor a csúcsesemény bekövetkezik, de amelyek közül bármelyik esemény be nem következésekor a csúcsesemény sem következik be.

A minimális vágatokhoz hozzárendelhetjük a bennük szereplő elemi események bekövetkezési valószínűségének szorzatát. Ekkor a minimális vágatokat érték szerint sorba rendezve megállapíthatjuk, hogy elsősorban melyik elemi események felelősek a csúcsesemény bekövetkezéséért.

A minimális vágatok további elemzésével megállapítható, hogy minimálisan hány hiba szükséges a csúcsesemény bekövetkezéséhez. Ez azért fontos jellemző, mert sok esetben a rendszerekkel szembeni meghibásodási valószínűségi követelményeket kiegészítik azzal, hogy a rendszer legyen legalább egyszeresen hibatűrő, vagyis egy hiba, bármilyen kis valószínűséggel is következne be, ne okozhassa a rendszer hibás reakcióját.

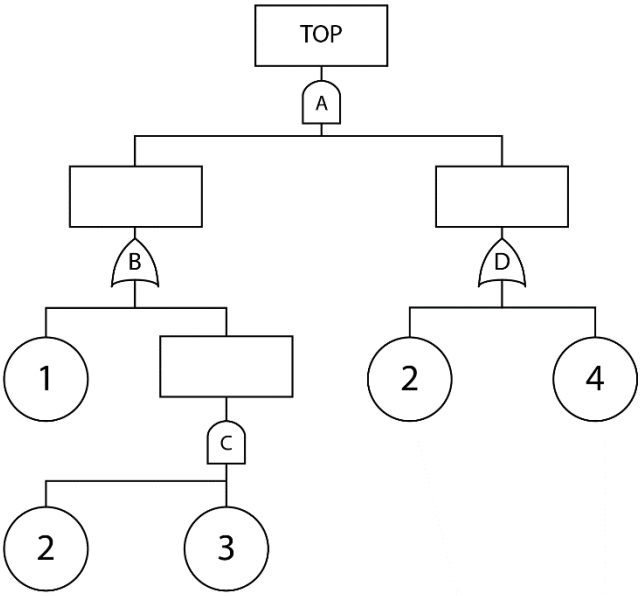
Amint az előző fejezetben láttuk, az egyes minimális vágatokhoz hozzárendelt számszerű eredmények összege nem a helyes végeredményt adja a csúcsesemény bekövetkezése szempontjából. Ennek egyik oka lehet, hogy az egyszerűsített számolási technika alkalmazása esetén egyes tagok elhanyagolásával csökkentjük a számítási feladatokat. Másik ok lehet az, hogy a minimális vágatokban többször is szerepelhetnek (természetesen különböző kombinációkban) olyan elemi események, melyek a hibafában csak egyszer szerepelnek (az egyes minimális vágatokhoz tartozó értékek a többi minimális vágattal való kapcsolat értékeit is tartalmazzák). Így tehát a minimális vágatokhoz tartozó számszerű valószínűségek csak összehasonlításra használhatók.

A minimális vágatok meghatározásának jól definiált algoritmusa van, melynek lépései az alábbiak.

Minimális vágatok meghatározásának módszere

1) Kizárólag az elemi eseményeket vesszük figyelembe, a fa összes többi elemét figyelmen kívül hagyjuk.
2) Közvetlenül a csúcsesemény alatt kezdve, minden kapuhoz egy egyedi karaktert rendelünk (egy nagybetűt), és minden elemi eseményhez egy egyedi számot rendelünk.
3) A csúcseseménytől kiindulva, lefelé haladva a fán, felépítünk egy kezdeti mátrixot az előző lépéshez hozzárendelt számokból és betűkből. A csúcseseményt reprezentáló karakter lesz a mátrix első eleme. Ezután sorban haladva az elemeken, végigiterálunk a mátrixon az alábbiak szerint.
    a. **ÉS** kapu esetén az egyes betűket lecseréljük a kapu bemenetén található számokkal, illetve karakterekkel, és ezeket a mátrixban horizontálisan helyezzük el.
    b. **VAGY** kapu esetén az egyes betűket lecseréljük a kapu bemenetén található betűkkel és számokkal, és ezeket a mátrixban vertikálisan helyezzük el. Minden újonnan létrehozott VAGY kapuból származó új sornak a mátrixban tartalmaznia kell az eredeti, transzformálás előtti sorban található elemeket is.
4) Végeredményként egy olyan mátrixot kapunk, mely már csak számokat tartalmaz, melyek elemi eseményeket reprezentálnak. Az ebben a mátrixban lévő sorok ún. logikai vágatokat alkotnak (Boolean-indicated cut set).
5) A minimális vágatok meghatározásához vizuálisan értékeljük ki a kapott mátrixot, és minden olyan sort eltávolítunk, amelyben csak olyan számok szerepelnek, amelyek már mind szerepelnek az azt megelőző sorok valamelyikében. Végül eltávolítjuk minden sorból az ismétlődő elemeket, és az ismétlődő sorokat is. Az így kapott mátrix sorai alkotják a minimális vágatokat.

A fent leírt folyamatra mutat példát az következő két ábra.

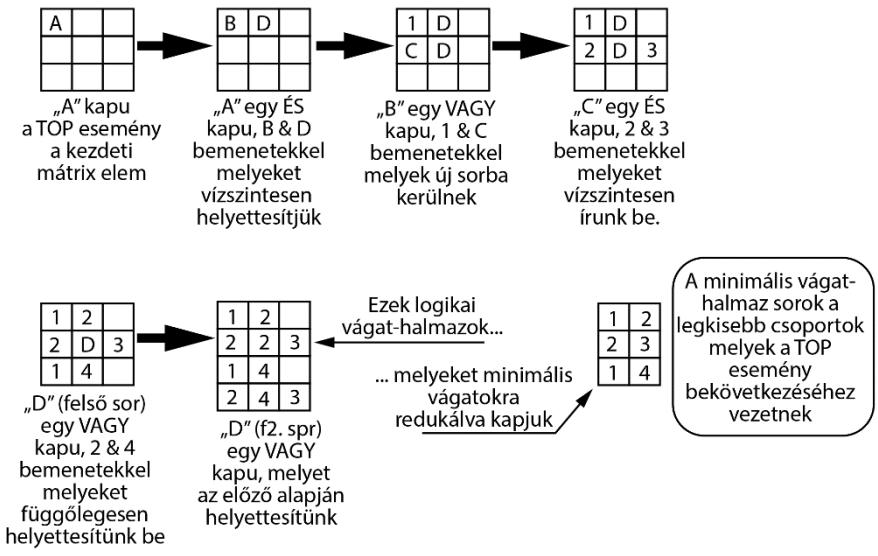


6.8. ábra. Hibafa generálásának első lépése.

Minimális vágatok kiértékelése, alkalmazása

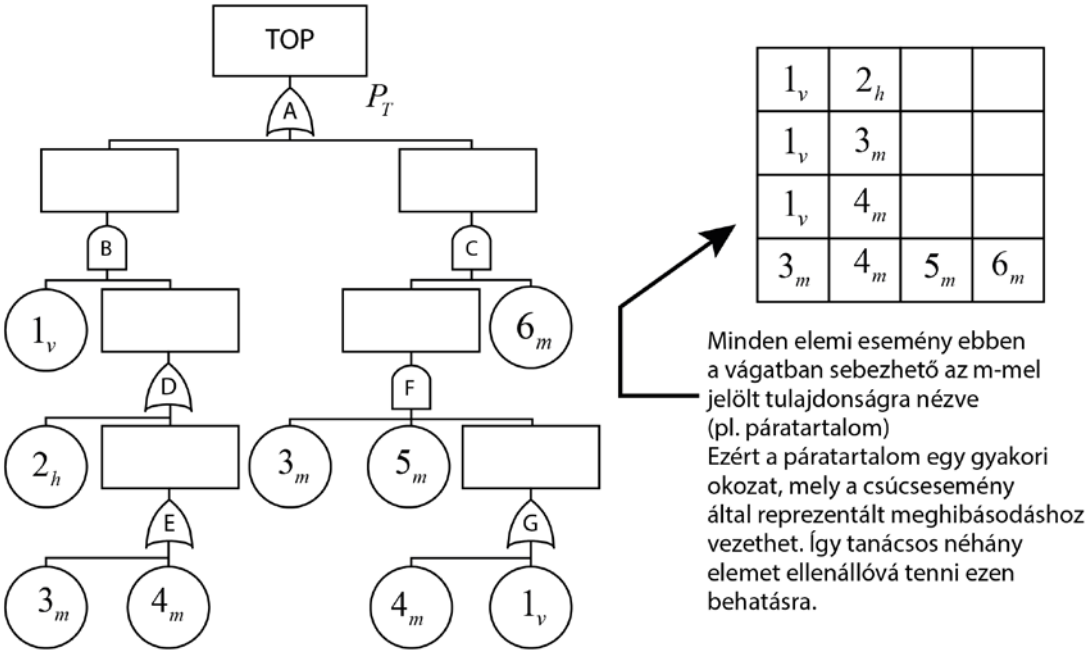
Az alábbiakban az előző 5 lépésben meghatározott minimális vágatokat elemezzük tovább és kifejtjük alkalmazási lehetőségeiket.

1) Mivel egy vágat azon elemi események egy csoportját jelenti, melyek együttes bekövetkezése a csúcsesemény bekövetkezését vonja maga után, egy vágat bekövetkezési valószínűsége (tehát annak a valószínűsége, hogy a halmaz a csúcseseményt indukálja) matematikailag teljesen hasonlóan fejezhető ki, mint az ÉS kapuk esetében, azaz n elemű vágat esetén:



6.9. ábra. A vágatok és a minimális vágatok meghatározásának egyes lépései az előző ábrán lévő példában.

2) A gyakori sérülékenységi okok feltárása. Ezt úgy tehetjük meg, hogy minden számozott elemhez (elemi események) alsó indexbe hozzárendeljük az arra az elemre jellemző sérülékenységet (pl. m – páratartalomra, q – melegre, v – rázkódásra stb.). Természetesen egy elemi eseményhez több ilyen sérülékenységet is rendelhetünk. Ezután megnézzük, hogy a minimális vágataink közül van-e olyan, amelyikben minden elem ugyanazt az alsó indexben lévő karaktert tartalmazza. Ha igen, akkor a csúcsesemény is sérülékeny lesz az e karakter által reprezentált fenyegetettségre. Erre mutat példát a 6.10. ábra, ahol a negyedik minimális vágat jelzi, hogy a csúcsesemény meghibásodását okozhatja a magas páratartalom.
3) Mindegyik előző lépésben beazonosított gyakori okozatra meghatározzuk annak valószínűségét.
4) Meghatározzuk a vágatok strukturális szignifikanciáját, kvalitatív rangsorolással, melyet az alábbi módon végzünk:
    a. Sok elemből álló vágat alacsony sérülékenységet jelez.
    b. Kevés elemből álló vágat magas sérülékenységet jelez.
    c. A nagyszámú vágat magas sérülékenységet jelez.
    d. Egy olyan vágat, mely egyetlen elemet tartalmaz, potenciális „egypontos” meghibásodást jelez, tehát olyat, mely egyetlen eseménytől is bekövetkezhet.



6.10. ábra. A gyakori sérülékenységi okok feltérképezésének menete.

5) Megbecsüljük minden egyes K vágatra annak ún. kvantitatív jelentőségét (Quantitatice Importance), I_K -t, melyet az alábbi képlet definiál:

$$I_K = P_K / P_T$$

ahol P_K annak a valószínűsége, hogy a vágat bekövetkezik (lásd a (6) pontot), és P_T pedig a csúcsesemény bekövetkezési valószínűsége.

6) Megbecsüljük minden e elemi eseményre annak ún. elem jelentőségét (Item importance), I_e -t az alábbi módón:

$$I_e = \sum_{e}^{N_e} I_{K_e} \tag{6.7}$$

ahol N_e jelöli azon minimális vágatok számát, melyek tartalmazzák az e iniciátortelemi eseményt, és I_{K_e} pedig azon minimális vágatok jelentőségét jelenti, melyek tartalmazzák az e elemi eseményt. Ezt szemlélteti a 6.11. ábra.

Minimális Cut Set (vágat)

1	2		
1	3		
1	4		
3	4	5	6

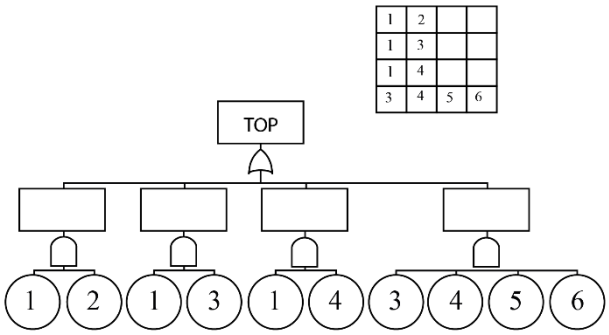
$$I_1 = \frac{(P_1 \times P_2) + (P_1 \times P_3) + (P_1 + P_4)}{P_T}$$

6.11. ábra. Példa az elem jelentőség számítására az 1-es elem esetén.

6.4 Minimális vágatok használata ekvivalens fák készítésére

A minimális vágatok felhasználásával lehetővé válik felépíteni a hibafát, mely felépítés azonban általában nem egyezik azzal, melyből az elemzés során kiindultunk. Azonban az itt leírt módszert követve a két fa matematikailag teljesen ekvivalens, így mindkettőn végzett elemzés ugyanazt az eredményt szolgáltatja. Az ilyen fajta újbóli konstrukció ereje abban rejlik, hogy sok esetben (bár nem mindig és nem garantáltan) a kiindulási fánál egyszerűbb struktúrát kapunk, melyen a további analízisek egyszerűbbé válnak.

Ez a rekonstrukció egyszerűn az egyes minimális vágatokat veszi alapul, és mindegyik vágatban lévő elemeket **ÉS** kapuval kapcsolja össze. Ez alkotja a fa alsó szintjét, majd az ezen a szinten lévő közbülső elemeket **VAGY** kapukkal összekapcsolva jut el a csúcseseményhez. Mivel az így létrejött fa csak két szintet tartalmaz, sok esetben egyszerűsíti az analízist az ilyen fajta átalakítás. Ezt a fajta átalakítást mutatja az alábbi ábra, mikor a végeredmény egy egyszerűbb struktúra.



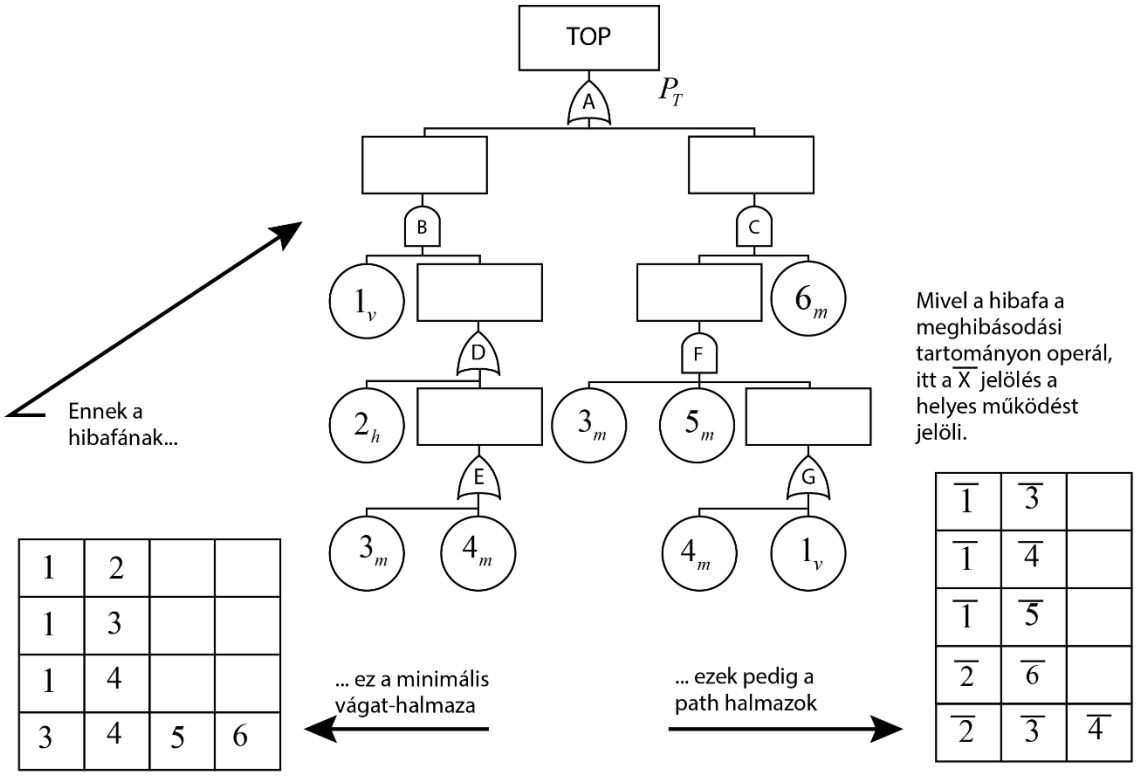
6.12. ábra. Minimális vágatok halmazával ekvivalens hibafa felépítésének menete.

6.5 Path halmazok meghatározása

Ahogy korábban is említettük, az ún. path halmazok a hibafa elemi eseményeinek egy olyan halmazát jelölik, melyek közül ha egyik sem következik be, az biztosítja, hogy a csúcsesemény sem fog bekövetkezni. Ezen halmaz szoros összefüggésben van a vágatok halmazával, és főként arra használjuk, hogy a hibafát megbízhatósági diagrammá alakítsuk át. E halmaz létrehozásának lépései:

1) A hibafában minden ÉS kaput VAGY kapura, illetve minden VAGY kaput ÉS kapura cserélünk.
2) A vágatok mátrixánál ismertetett módszerrel kialakítjuk a végső mátrixot, melynek minden sora egy-egy path halmazt tartalmaz.

A kétféle halmaz létrehozását mutatja be a következő ábra egy egyszerű példán keresztül.



6.13. ábra. Cut és path halmazok létrehozása egy egyszerű példán keresztül.

6.6 Érzékenységvizsgálatok (fontosságvizsgálatok)

Az érzékenységvizsgálatok arra adnak választ, hogy mennyire érzékeny a csúcsesemény előfordulási gyakorisága az egyes paraméterek értékeinek megváltoztatására. Az egyes paraméterek alatt az egyedi alkatrész-meghibásodásokhoz tartozó valószínűségi modellek paramétereit (λ, μ vagy TR, TI, TF) értjük. Ezt a tervezőnek azért kell ismernie, mert így választ lehet kapni arra a kérdésre, hogy milyen paraméterek változtatásával (javításával) lehet a csúcseseményre vonatkoztatott jellemzőket befolyásolni.

A vizsgálat elvégzéséhez a vizsgálni kívánt paraméter értékét előbb n-szeresére, majd az eredeti paraméter n-ed részére változtatják, és kiszámolják a csúcsesemény rendelkezésre nem állásának értékeit (Q_{max} és Q_{min}) úgy, hogy közben a többi paramétert állandó értéken tartják. A Q_{max} / Q_{min} hányados értéke mutatja azt, hogy a paraméter megváltoztatásával mennyire változnak a globális jellemzők. Az összes paraméterre elvégezve a vizsgálatot a paraméterek fontossági rangsorát állíthatjuk fel.

Az érzékenységvizsgálatokkal nem csak az egyes meghibásodási ráták változásának hatása térképezhető fel, de választ kapunk az egyes definiált időintervallumok (tesztelési idők, javítási idők) változtatásának hatásaira is. Ez igen fontos lehet a tervezőmérnök számára, hiszen a rendszer jellemzőinek egyik javítási módja (amennyiben nem akarunk, vagy nem tudunk jobb, megbízhatóbb komponenseket használni) a tesztelések gyakoribb lefolytatása (ami a hibák hamarabbi felfedését eredményezi), illetve a javítási idő csökkentése.

Az érzékenységvizsgálatok másik típusánál nem az elemi eseményekhez tartozó paramétereket változtatják, hanem az elemi esemény rendelkezésre nem állásának értékét befolyásolják közvetlenül. Ha az értéket konstans 1-nek feltételezzük, azt az esetet kapjuk, amikor az egyedi komponens meghibásodása mellett üzemel a rendszer, és erre az esetre számíthatjuk ki a csúcsesemény rendelkezésre nem állását. (Ha az ilyenkor kiszámolt rendelkezésre nem állás értéke 1, az azt jelenti, hogy a komponens meghibásodása a teljes rendszer hibájához vezet, vagyis a rendszer nem tesz eleget az egyszeres hibatűrés feltételének.)

Amennyiben az elemi esemény túlélési valószínűségét választjuk 1-nek, azt az elméleti esetet kapjuk, amelynél az alkatrész soha nem hibásodik meg, tehát ideális. Az ilyenkor kiszámolt csúcsesemény paraméterek azokat a határokat mutatják meg, amelyek az elemi esemény (alkatrész) paramétereinek változtatásával maximálisan elérhetőek.

A hibafa számszerűsítése nemcsak a rendszermegbízhatósági paraméter értékét adja meg, hanem a rendszermegbízhatósági paramétert kisebb-nagyobb mértékben befolyásoló egyéb tényezőkről is szolgáltat információt. Ez azt jelenti, hogy gyakran meghatározható az, hogy egy adott változtatás a rendszerben ténylegesen hozzájárul-e a megbízhatóság javításához vagy sem. Például a működési igénytől függő meghibásodás valószínűségének csökkentéséhez felesleges célul tűzni az E1 feszültségforrás helyreállítási idejének csökkentését. A helyreállítási idő felére való csökkentésének (pl. tartalék feszültségforrás alkalmazása) gyakorlatilag nincs hatása a rendszerre értelmezett működési igénytől függő meghibásodás valószínűségére.

A példában szereplő biztonsági rendszer esetében a működési igénytől függő meghibásodás valószínűségét leginkább meghatározó elemek az érzékelők és az egy-a-kettőből logikai elem. A

rendszerelem adatainak vagy a hibafa-modellnek a megváltoztatásából vagy módosításából eredő hatások értékeléséhez érzékenységi elemzéseket végeznek.

Az érzékenységi elemzés során ezeknek a változóknak különböző értékeket adhatunk, és így meghatározhatjuk a végeredményekben megmutatkozó eltéréseket. Az érzékenységi elemzések egyik típusa az, amikor a kiértékelést úgy végezzük el, hogy a hibafa egyik alapeseményéhez az egyik esetben nagy, a másik esetben kis értékű meghibásodási rátát rendelünk. Amennyiben a kiszámított rendszer-megbízhatósági paraméter nem változott számottevően, akkor ez az alapesemény nem bír nagy jelentőséggel és nem szükséges további figyelmet fordítani rá. Amennyiben viszont a rendszermegbízhatósági paraméter változása jelentős mértékűre adódott, akkor pontosabb adatokat kell szerezni vagy az eseményt további alapokokra kell bontani.

A mintapéldában szereplő biztonsági rendszer esetében ha a vizsgálati intervallumot az évenkénti 4 alkalomról 8 alkalomra növeljük, akkor az érzékelőkre vonatkozó működési igénytől függő meghibásodás valószínűsége 2,1E-04 értékről 9E-05-re csökken, és ezzel a működési igénytől függő meghibásodás valószínűsége a teljes rendszerre 2,4E-04 lesz.

A fenti számítások pontértékeken alapulnak. A valóságban a kiszámítandó rendszermegbízhatósági paraméterek számértékei bizonytalan értékek. Ez azt jelenti, hogy valamilyen valószínűségi eloszlással jellemezhetők, és az elvégzett elemzések csak átlagos értékeket adhatnak. Hangsúlyozzuk, hogy mennyiségi megbízhatóság-elemzés során kiszámított pontértékeket nem szabad rögzített számértékeknek venni. Egy adott rendszermegbízhatósági paraméter kiszámított értéke mindig becsült érték, melynek szórása van. A bemenő paraméterek bizonytalansági mérőszámai alapján a kiszámított rendszermegbízhatósági paraméter bizonytalansága becsülhető. E bizonytalanság meghatározásához a legelterjedtebben alkalmazott módszer a Monte Carlo szimuláció.

6.7 MATLAB implementáció

Az irodalmi feldolgozás során a megismert módszerek és algoritmusok alapján elkészítettünk egy olyan gyorsan és egyszerűen működő, MATLAB környezetben futó programot, mely néhány kezdeti paraméter megadása után képes meghatározni a minimális vágat és path halmazokat, illetve kiszámolni a csúcsesemény bekövetkezési valószínűségét. A program, mely az FTA_v02.m fájlban található, a 1. kódrészletben látható egyszerű példa elemzésével mutatjuk be. Az alábbi kódrészletben látható, hogy milyen kezdeti paraméterekre van szüksége az algoritmusnak.

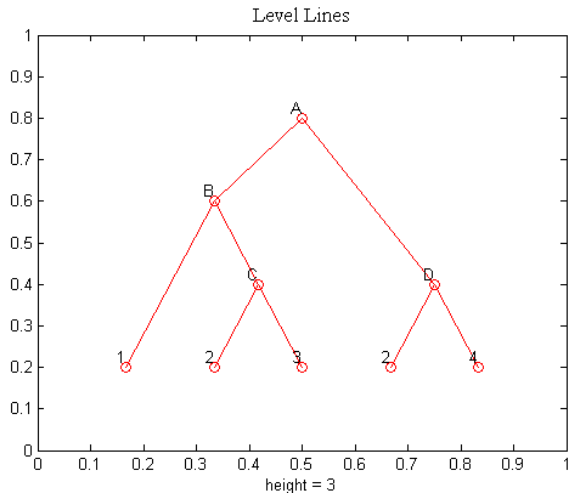
```
1. %bemeneti adatok
2. treeVec=[0 1 2 2 4 4 9 9 1]; %favektor
3. par={'es','or','es','or'}; %az egyes csomópontoknál álló kapuk
4.  esely=[0  0  0.1  0  0.05  0.2  0.05  0.01  0]; %az alapvető események
esélyei
5.  name1 = {'A'  'B'  '1'  'C'  '2'  '3'  '2'  '4'  'D'};   %fa pontjainak
elnevezése
```

1. Kódrészlet. Az FTA_V02.m program szükséges ezdeti paraméterei.

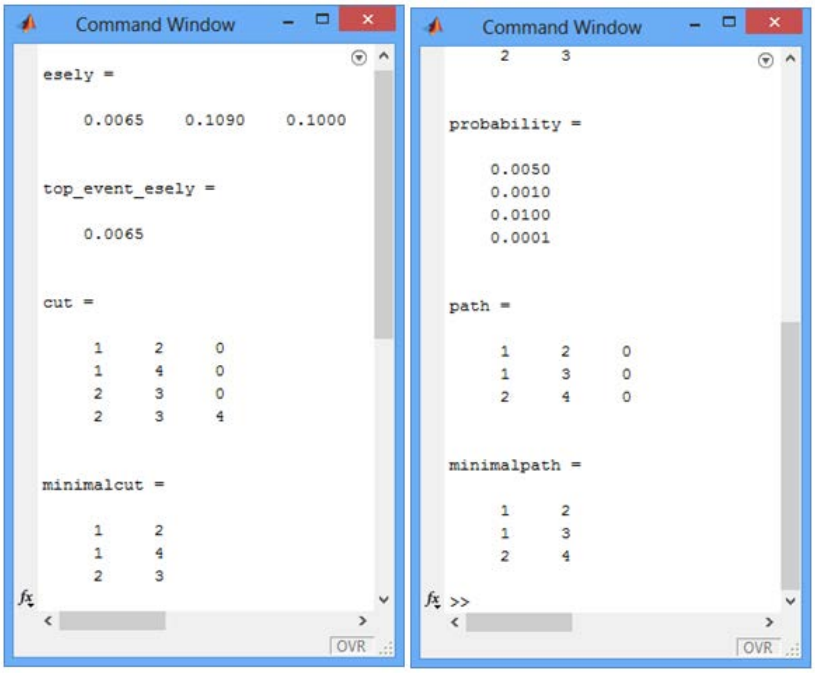
Az 2. sorban található tömb a felépítendő hibafa struktúráját tartalmazza. Itt az egyes számok az alábbi jelentéssel bírnak:

- A csúcseseményt minden esetben a 0 reprezentálja.
- Bármely más x szám az $x-1$ által reprezentált csomópont gyermeke.

A 3. sorban lévő vektorba kell megadnunk sorban az összeköttetéseket definiáló kapuk fajtáját, értelemszerűen „és” definiálja az ÉS kaput, és „vagy” a VAGY kaput. A 4. sorban látható „esely” változóban kell elhelyeznünk minden egyes csomóponthoz az alkalmazandó valószínűségeket, amit a kapuk esetében 0-ra veszünk. Az 5. sorban látható tömbben pedig a fa pontjainak elnevezéseit kell megadnunk, a korábban a fa felépítésénél ismertetett módon, tehát a kapukat betűkkel, míg a csomópontokat számokkal reprezentálva. Látható, hogy a 6.8 ábrán lévő fa paramétereit tartalmazza a kódrészlet. A programot futtatva, az megjeleníti nekünk a fa vizuális reprezentációját, amint az alábbi ábrán látható.



6.14. ábra. A MATLAB program futásának eredménye, a hibafa vizuális reprezentációja.



6.15. ábra. A MATLAB program által szolgáltatott eredmények, két részletben megjelenítve.

A programot futtatva, az szövegesen szolgáltatja az eredményeket, amint a 6.15 ábrán látható. A parancssorban először kiírja az alkalmazott valószínűségeket (melyeket paraméterként megadtunk - esely), majd a csúcsesemény bekövetkezési valószínűségét, melyet kiszámolt (top_event_esely). Eztán megjeleníti a vágatok halmazait tartalmazó mátrixot (cut), majd a minimális vágatokat

tartalmazó mátrixot is (minimalcut). Végül megjeleníti a kiszámolt valószínűségeket a közbülső elemekre (probability), és megadja a path halmazokat (path) és a minimális path halmazokat (minimalpath) reprezentáló mátrixokat is.

6.8 Összefoglalás

A hibafa elemzés során tehát egy ún. csúcsesemény, mely valamilyen súlyos meghibásodást vagy valamilyen más nem kívánt eseményt jelöl, meghibásodási valószínűségét becsüljük az elemi eseményekből kiindulva. A fát fentről lefelé építjük fel, majd alulról haladva értékeljük ki, melynek során meghatározzuk azon események halmazát, melyek együttes bekövetkezése garantálja a csúcsesemény bekövetkezését. Ezután képesek vagyunk jó közelítéssel becsülni a csúcsesemény bekövetkezési valószínűségét. Az alábbiakban a rendszer előnyeit és hátrányait foglaljuk össze.

6.8.1 Előnyök

1) Lehetővé teszi a kombinált hibák/meghibásodások valószínűségeinek kiértékelését komplex rendszereken.
2) „Egypontos” és gyakori meghibásodási okozatok feltárását, kiértékelését teszi lehetővé.
3) Használatával egy rendszert újrakonfigurálva csökkenthető annak sérülékenysége.
4) Segítségével beazonosíthatók a sebezhetőségek és az olcsó ellenintézkedések, így az erőforrások vezetett fejlesztésével csökkenthető a kockázat.
5) Path halmazok alkalmazhatók gazdasági kimutatásokban, összehasonlítva a csökkentett meghibásodási valószínűségek nyereségét az ellenintézkedések beruházási költségével.

6.8.2 A módszer korlátai

1) A csúcsesemény csak egyetlen nem kívánt eseményt reprezentál, így egy komplex rendszer esetén több hibafa elemzés szükséges.
2) Egy ilyen valószínűségeken alapuló elemzés általában sok időt és erőforrást igényel.
3) Csak abban az esetben hatékony a hibafa, ha minden szükséges résztvevőt, akik meghibásodást okozhatnak, bevonunk.
4) Bármely két eseménynek, amely ugyanahhoz a logikai kapuhoz kapcsolódik, függetlennek kell lennie.
5) Bármely szinten lévő esemény vagy feltétel független kell legyen a következő szinten elhelyezkedő eseményektől és feltételektől.
6) Ha nem azonosítjuk a gyakori meghibásodási okozatokat, akkor a hibafa hibás eredményeket adhat.
7) Minden elemi esemény valószínűségének konstansnak és előre jelezhetőnek kell lennie.

7 Sikerfa-elemzés (Success Tree Analysis- STA)

A sikerfa elemzés egy visszafele haladó (top-down) szimbolikus logikai modell, amelyet az FTA-tól eltérően nem a meghibásodási, hanem a sikerességi tartományban definiálunk és generálunk. Az elemzés során itt a csúcseseményből kiindulva, amely valamilyen várt eseményt, helyes működést reprezentál haladunk a rendszer elemi sikeres eseményei felé, melyek okozati elemekként működnek. Gyakorlatilag az STA az FTA elemzés logikai komplemenseként definiálható, hiszen itt a sikertartományban dolgozva elemezzük a helyes működés valószínűségét, míg FTA esetén a hibatartományon elemezve jutunk el a meghibásodás bekövetkezésének valószínűségéhez.

Az STA során, teljesen hasonlóan FTA-hoz, felépítjük a sikerfát, meghatározzuk az egyes elemi eseményeknél a helyes működés valószínűségét, ezeket a valószínűségeket felhasználva kalkuláljuk ki a csúcsesemény bekövetkezési valószínűségét, valamint itt is meghatározzuk a vágat (cut) és path halmazokat. A sikertartományban számolva vágatok halmazának az elemi események egy olyan halmazát nevezzük, melyek közül ha mindegyik bekövetkezik, az kizárja a csúcsesemény bekövetkezését, tehát ha egy vágatban minden elem, berendezés helyesen működik, akkor a csúcsesemény, a fő berendezés nem fog helyesen működni. A minimális vágat a vágatok halmazából a legkevesebb elemet tartalmazó halmaz. Path halmaznak itt az iniciátorok olyan halmazát nevezzük, melye mindegyikének bekövetkezése magával vonja a csúcsesemény bekövetkezését is.

Egy esemény sikerességét (helyes működésének esélyét) a sikeres (helyes) működések és az összes kísérletek számával definiáljuk.

$$P_S = \frac{S}{S+F} \tag{7.1}$$

ahol S a sikeres kísérletek (helyes működés) száma, F pedig a meghiúsult kísérletek (helytelen, hibás működés, meghibásodás) száma. Jelen esetben a megbízhatóságot egyszerűen definálhatjuk:

$$R = P_S \tag{7.2}$$

STA-t is különösen olyan rendszerekben alkalmaznak, melyeknél magas a komoly baleseti kockázattal járó események, tevékenységek száma, mellyel biztosítható, hogy a az alkalmazott ellenintézkedések együttesen sikeres csúcseseményhez vezetnek. Ez a technika általánosan használható komplex rendszerek esetén, mind hardware mind nem hardware elemekből felépülő rendszereknél. STA-t általában a projektek tervezési-fejlesztési fázisában használnak, de néha a gyártás-integráció- teszt-értékelés fázisban is helyet kap. Sokszor használják az FTA során létrehozott hibafa validálására, mivel a két analízis egymás logikai komplemenseként kezelhető, így bármelyik érvényessége esetén a másiknak is annak kell lennie.

7.1 Az elemzés folyamata, példa

A sikerfát a hibafához hasonlóan különböző események és logikai kapuk kapcsolatából építhetjük fel. A használható szimbólumok listáját itt is az 6.1. táblázat. Hibafa felépítéséhez használható szimbólumok és azok leírása. tartalmazza. Bár számos szimbólum áll rendelkezésre, az esetek nagy többségében elegendő az alábbi 4 szimbólum:

1) csúcsesemény és köztes események szimbóluma

2) VAGY kapu
3) ÉS kapu
4) elemi esemény

Ezek használatával a sikerfa felépítésének folyamata teljes egészében megegyezik az 6.1. ábrán látható, a hibafa felépítésének miként jével.

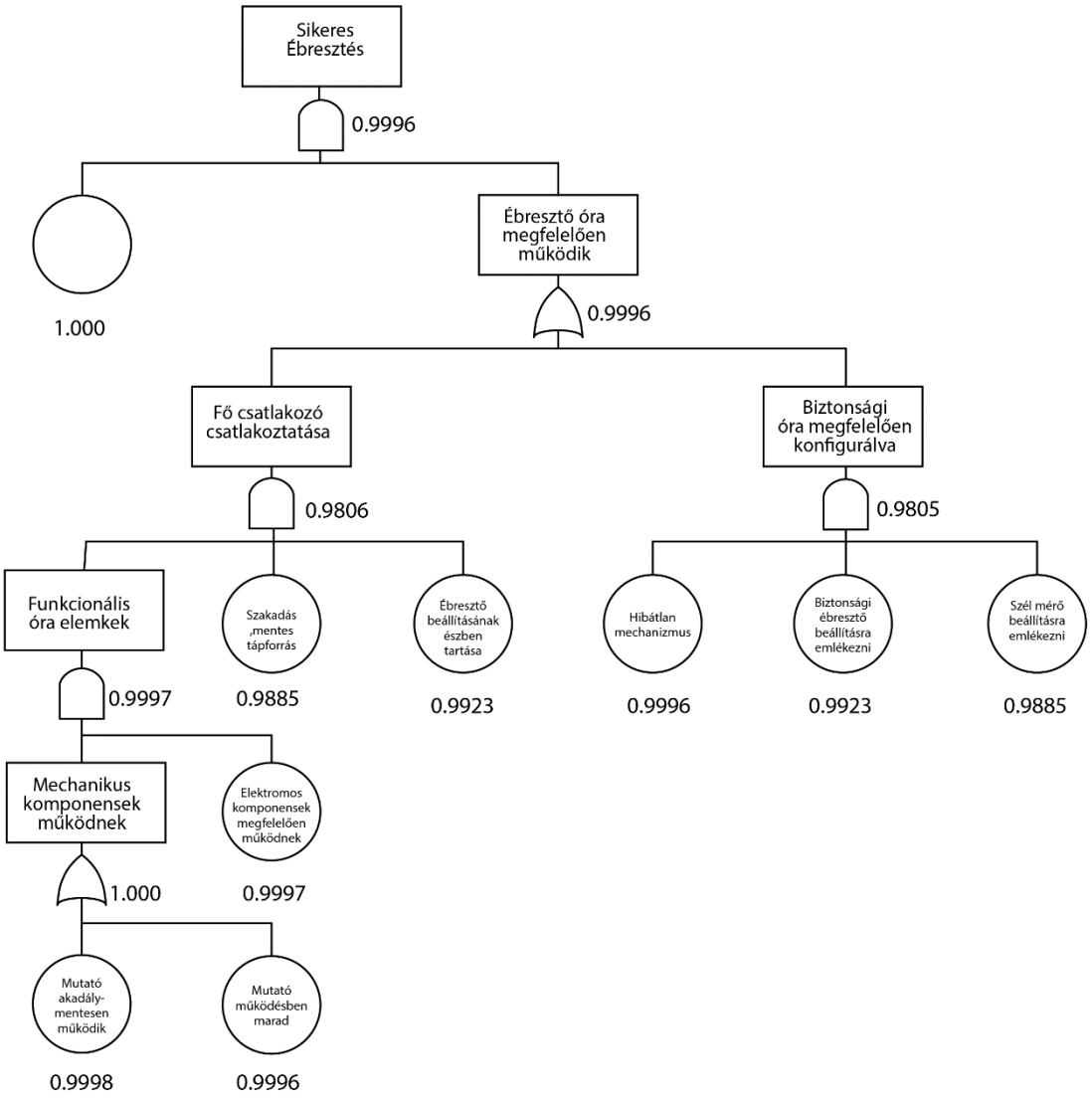
A hibafa (mivel ahogy említettük, szoros összefüggésben van a sikerfával) áttranszformálható sikerfává, egyszerűen csak minden ÉS kaput OR kapura, és minden OR kaput ÉS kapura kell változtatnunk a fában, és újra kell inicializálnunk minden elemi eseményt, közbenső- és csúcseseményt, hogy meghibásodás helyett helyes működést reprezentáljon.

Első lépésként tehát most is meg kell határoznunk minden elemi eseményhez a siker valószínűségét (P_S). Ezek meghatározása történhet gyártói kézikönyvekből, adatokból, ipari szabványokból, katonai szabványokból, historikus adatokból, vagy szimulációk és tesztelések eredményeiből. Ugyancsak használható itt is a log-átlag metódus, melyet a 6.4. ábra szemlélteti. természetesen itt is igaz, hogy a megbízhatóság éppen a meghibásodás komplementere, vagyis:

$$R = P_S = 1 - P_F \tag{7.3}$$

Az elemi események bekövetkezési valószínűségeinek meghatározása után ezen valószínűségek tovább terjedését kell meghatároznunk, mely ugyancsak megegyezik az FTA elemzésnél ismertetettel, a legfontosabb egyenleteket a 6.2. táblázat tartalmazza. A vágatok halmazának és a path halmazok meghatározása is az FTA-nál ismertetett módon történik, amit a 6.4 és 6.5 fejezetekben ismertettünk.

Egy példa sikerfa látható a 7.1. ábrán, mely a 6.10. ábrán bemutatott hibafának felel meg.



7.1. ábra. Példa sikerfa, mely a 6.10 ábrán látható hibafának felel meg.

7.2 Összefoglalás

A sikerfa elemzés során tehát egy ún. csúcsesemény, mely valamilyen kívánt, sikeres működést jelöl, helyes működési valószínűségét becsüljük. A fát fentről lefelé építjük fel, majd alulról haladva értékeljük ki, melynek során meghatározzuk azon események halmazát, melyek együttes bekövetkezése garantálja a csúcsesemény bekövetkezését. Az elemzés teljesen megegyezik a hibafánál tárgyalt módszerrel, a létrejött sikerfa gyakorlatilag a hibafa logikai komplementere.

7.2.1 Előnyök

1) Használatával kiértékelhető a rendszer üzemeltetéséből származó várt, vagy helyes működés valószínűsége.
2) Kiegészíti a hibafát oly módon, hogy segítségével ellenőrizhetjük a hibafa logikai helyességét.

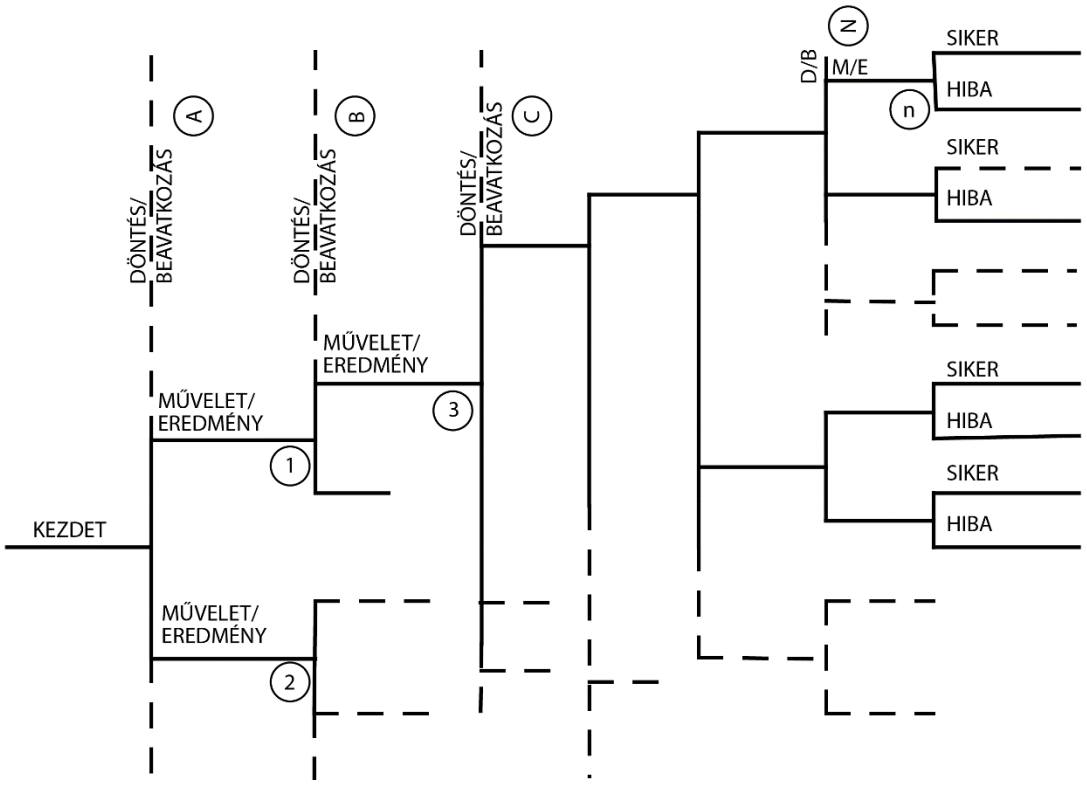
7.2.2 A módszer korlátai

1) A csúcsesemény csak egyetlen kívánt eseményt reprezentál, így egy komplex rendszer esetén több sikerfa elemzés szükséges.

2) Egy ilyen valószínűségeken alapuló elemzés általában sok időt és erőforrást igényel.
3) Csak abban az esetben hatékony a sikerfa, ha minden szükséges résztvevőt akik a helyes működéshez, sikerhez vezethetnek, bevonunk.
4) Bármely két eseménynek amelyik ugyanahhoz a logikai kapuhoz kapcsolódik, függetlennek kell lennie.
5) Bármely szinten lévő esemény vagy feltétel független kell legyen a következő szinten elhelyezkedő eseményektől és feltételektől.
6) Minden elemi esemény valószínűségének konstansnak és előre jelezhetőnek kell lennie.

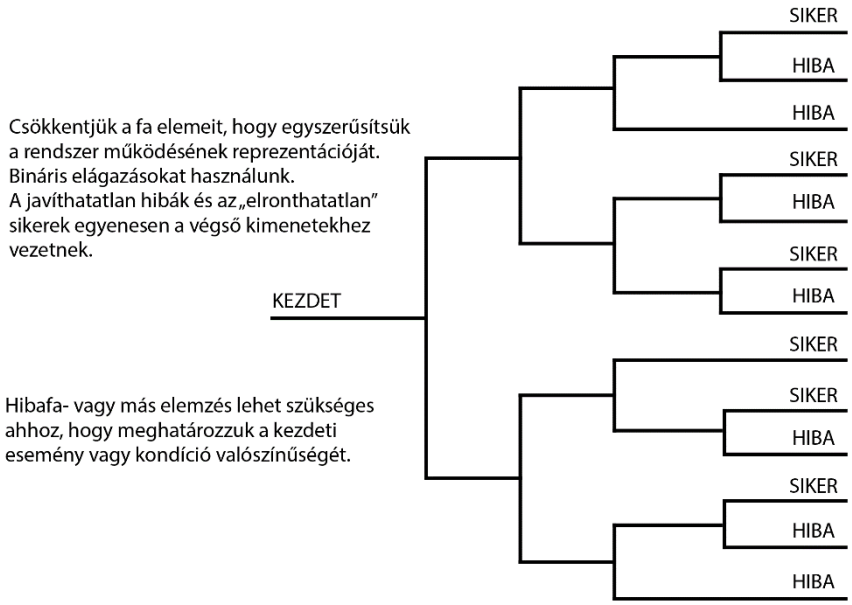
8 Eseményfa-elemzés (Event Tree Analysis- ETA)

Az eseményfa elemzés [1] [3] egy előre haladó (bottom-up), lentről felfele építkező szimbolikus logikai modell, melyet mind a meghibásodási-, mind a sikertartományban generálunk. Az eseményfa lényegében egy feltételezett kezdeti esemény által kiváltott védelmi működések kvalitatív reprezentációja, egy bináris eseménylánc logika. A kezdeti esemény ebben az esetben lehet akár egy meghibásodás, vagy üzemzavar, de egy helyes, normális módon üzemelő berendezés is. Egy általános eseményfa a rendszer minden lehetséges működési útvonalát, sorozatát ábrázolja, a kezdeti eseményből kiindulva. Egy nagyon általános esetet mutat a 8.1. ábra.



8.1. ábra. Eseményfa, általános esetben. Minden lehetséges működési permutációt ábrázolunk. Mindegyik útvonal a fában valamilyen végső meghibásodáshoz vagy helyes működéshez vezet.

Bernoulli modell eseményfának nevezzük azokat az eseményfákat, melyek kizárólag bináris elágazásokat tartalmaznak, így jelezve, hogy a rendszer minden lépésben vagy sikeres vagy hibás műveletet hajt végre. Egy ilyen eseményfa látható a 8.2. ábrán. Az olyan speciális eseményfákat, melyek csak nullákat és egyeket tartalmazhatnak az egyes események és egységek kimenetein, döntési fáknak nevezzük.



8.2. ábra. Bernoulli modellt használó eseményfa.

Az ETA módszer különösen alkalmas katasztrófa-elhárító rendszerek, és tervezett biztonsági jellemzők elemzésére, de alkalmas működtetési eljárások, menedzsment döntések, és egyéb nem hardware elemekből felépülő rendszerek elemzésére is. A módszert az 1970-es évek elején kezdték alkalmazni olyan megbízhatóságanalízis-munkáknál, ahol a teljes rendszer modellezése a később bemutatandó hibafákkal már kezelhetetlenül nagy modellekhez vezetett volna. Kombinálva az FTA technikával, szenzitivitás kiértékelések létrehozására is alkalmas. A módszert többször használják az FMEA metódus (Failure Mode and Effect Analysis = Hibamód és hatás elemzés) kiegészítéseként.

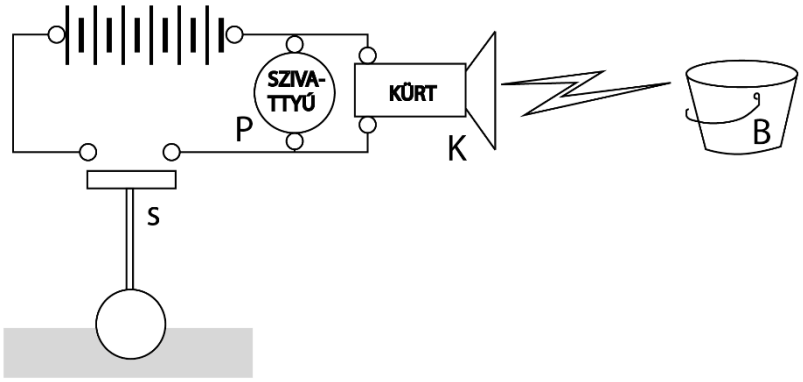
8.1 Az elemzés folyamata, példa

Az ETA elemzés lépései a következők:

1) Definiáljuk az eseményfa kiindulási pontját, a kezdeti eseményt (általában a vizsgált rendszer szempontjából külső esemény).
2) Meghatározzuk a kezdeti útvonalakat, tehát a fa kezdeti elágazásait, melyek valamilyen kétállapotú feltétel (pl. meghibásodás) teljesülésének vagy nem teljesülésének hatására történnek. Ezt a „Mi történik ha a rendszert kezdeti eseménynek tesszük ki?" kérdésre adott válasz definiálja. Általános jelölés, hogy a meghibásodást jelentő útvonal halad lefele a fában, míg a sikeres eseményt reprezentáló útvonal felfelé.
    a. Általános eseményfa esetén a rendszer minden lehetséges működési permutációját ezzel az elágazásos módszerrel elvezetjük egy sikeres vagy meghibásodásos leálláshoz.
    b. Bernoulli modell eseményfa esetén bináris elágazásokat használunk a rendszer útvonalainak kialakításához. Egyszerűsítjük a fát, a szükségtelen elágazások eliminálásával, tehát eltávolítjuk a javíthatatlan hibák és az „elronthatatlan" sikerek ágait.
3) FTA vagy más elemzéssel meghatározzuk a kezdeti esemény valószínűségét. Döntési fa esetén ezt egynek vesszük.

4) Meghatározzuk minden lehetséges útvonal valószínűségét, melyet az addig az útvonalon lévő egyes események valószínűségeinek szorzat ad.
5) Meghatározzuk a rendszer sikerességi valószínűségét, melyet a sikerben végződő útvonalak valószínűségeinek összegéből számolunk.
6) Meghatározzuk a rendszer meghibásodási valószínűségét, melyet a meghibásodásban végződő útvonalak valószínűségeinek összegéből számolunk.

Egy példa rendszer elemzésén mutatjuk be az eseményfa analízist. A rendszer az alábbi ábrán látható. A rendszer egy árvíz elleni védelmi rendszer. Emelkedő vízszint esetén az **S** úszókapcsoló megemelkedik, és zárja az áramkört, melynek hatására a **P** pumpa bekapcsol, melyet egy szünetmentes tápegység táplál. Az üzemeltetők figyelmeztetésére a K kürt is megszólal, mert amennyiben a szivattyú nem működne, a **B**-vel jelölt szereplő vödörrel avatkozik be. Mind a szivattyú, mint a vödrös megoldás hatékonyan csökkenti a vízszintet. Tegyük fel, hogy megkezdődött az árvíz, és elemezzük ETA módszerrel a rendszer lehetséges reakcióit!

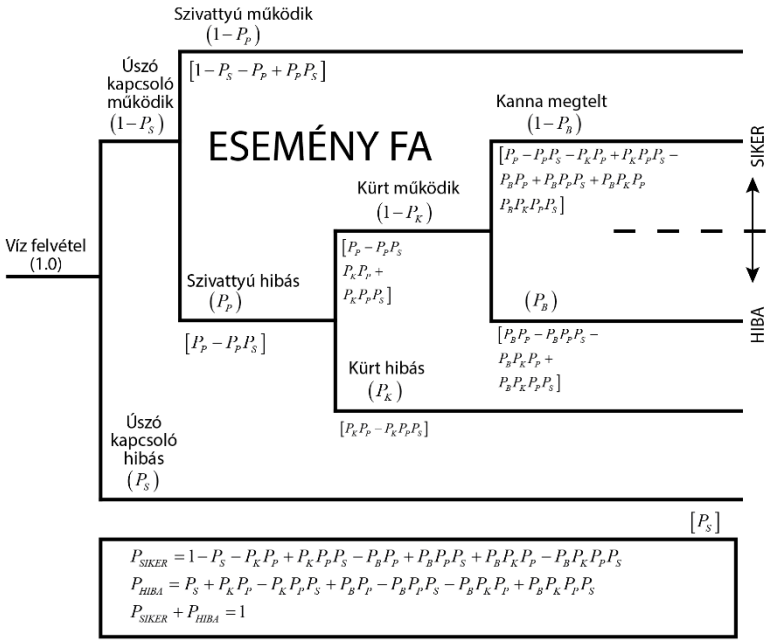


8.3. ábra. A példa árvízvédelmi rendszer sematikus ábrája.

Az elemzés során az alábbi feltevésekkel élünk.

- Az áramellátás minden időben, korlátlanul rendelkezésre áll.
- Csak a négy rendszerkomponenst kezeljük, melyek **S, P, K, B.**
- Az operátor hibáját figyelembe kell vennünk a **B** jelű szereplőnél.

A rendszerből felépíthető végső eseményfát a 8.4. ábra szemlélteti.



8.4. ábra. A példa alkalmazáshoz konstruált eseményfa.

Mivel a példa elején feltettük, hogy az árvíz bekövetkezett, így a kezdeti eseményünk valószínűsége 1, és a fent látható fa már szakértői beavatkozás után a legegyszerűbb formájában látható. Például, mivel az úszókapcsoló meghibásodása egy kijavíthatatlan meghibásodás, ennek az útvonala közvetlenül a végső meghibásodáshoz vezet, bármilyen közbülső utat kizárva. Hasonlóan, mivel az áramellátás mindig stabilan működik, annak helyes működését reprezentáló útvonal egyenesen a végső sikeres eseményhez vezet.

8.2 Összefoglalás

Az eseményfa (Eseményfa: Event Tree, ill. Eseményfa Analízis: Event Tree Analysis – ETA) tehát egy bináris döntési fa, amelynek célja egy kezdeti esemény különböző feltételek melletti hatásainak vizsgálata. Főként olyan megbízhatóságanalízis-munkáknál alkalmazzák, ahol a teljes rendszer modellezése a később bemutatandó hibafákkal már kezelhetetlenül nagy modellekhez vezetett volna. Valójában az eseményfa a közgazdaságtanban széleskörűen alkalmazott általános döntési fa adaptálása.

8.2.1 Előnyök

1) Egyszerre több, egyszerre jelen lévő rendszer-meghibásodást is kiértékelhető vele.
2) Szimultán működik a meghibásodási- és sikertartományon is.
3) Végső állapotokat is be kell vonni a módszerbe.
4) Feltárja a potenciális egypontos meghibásodásokat, a rendszer sérülékeny területeit, és az alacsony költségvetésű ellenintézkedéseket, így irányítottan oszthatók el a fejlesztések, erőforrások, mellyel javítható a kockázatok kordában tartása, és optimálható a szűkös erőforrások elosztása.
5) „Gyors és mocskos” összehasonlító technika, mely azonban nagyon tiszta képet ad a nem hatékony ellenintézkedésekről.

8.2.2 A módszer korlátai

1) Az elemzés csak egyetlen kezdeti esemény kezel, így egy komplex rendszer esetén több eseményfa elemzés szükséges.
2) A kezdeti eseményt nem az analízis határozza meg, hanem az analízist végzőnek kell előre tudnia.
3) A működési útvonalakat előre látnia kell az analízist végzőnek.
4) Bár általában az elemzés több meghibásodáshoz vezető útvonalat is azonosít, a veszteségek mértéke nem megkülönböztethető, így annak eldöntésére külön analízis alkalmazandó.

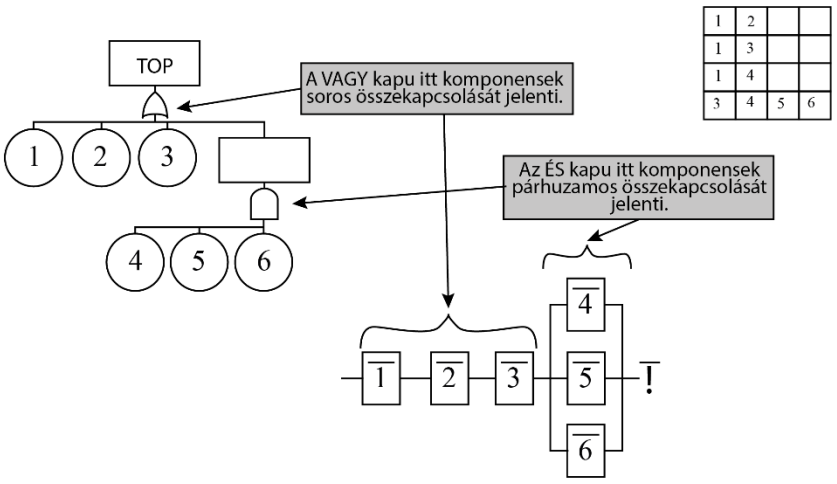
9 Hibafa, megbízhatósági blokk diagram és eseményfa transzformációk

Eddigi elemzéseinkből már tudjuk, hogy mind a hibafák, mind az RBD-k, mind az eseményfák logikai modellek. A hibafát a meghibásodási tartományon, a megbízhatósági blokkdiagramokat a sikerességi tartományon, az eseményfákat pedig mind a meghibásodási, mind a sikerességi tartományokon generáljuk. Az alábbiakban bemutatjuk, hogy ezen technikák közül bármelyik áttranszformálható a másik kettő bármelyikébe, ekvivalens logikai átalakítások alkalmazásával.

Ezen technikákkal az elemzők képesek a különböző módszerek előnyeit kihasználni. A hibafák széleskörű kvalitatív vagy kvantitatív elemzést nyújtanak az elemzőknek, a RBD-k egy egyszerűsített módszerrel reprezentálják a rendszerlogikát, míg az eseményfák lehetővé teszik a mérnökök számára, hogy mind a sikerességi, mind a meghibásodási tartományon dolgozzanak.

9.1 Hibafából RBD konverzió

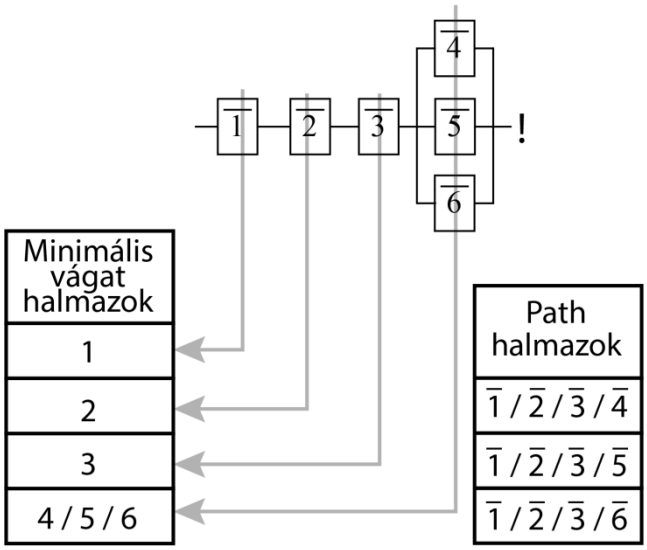
Amint már tudjuk az RBD a rendszer komponenseinek függvényeit tartalmazza, melyek ha érvényesek, helyes működést indukálnak a hibafa csúcseseményében. A hibafa-RBD konverzió látható a 9.1. ábrán.



9.1. ábra. Hibafa RBD-vé konvertálása.

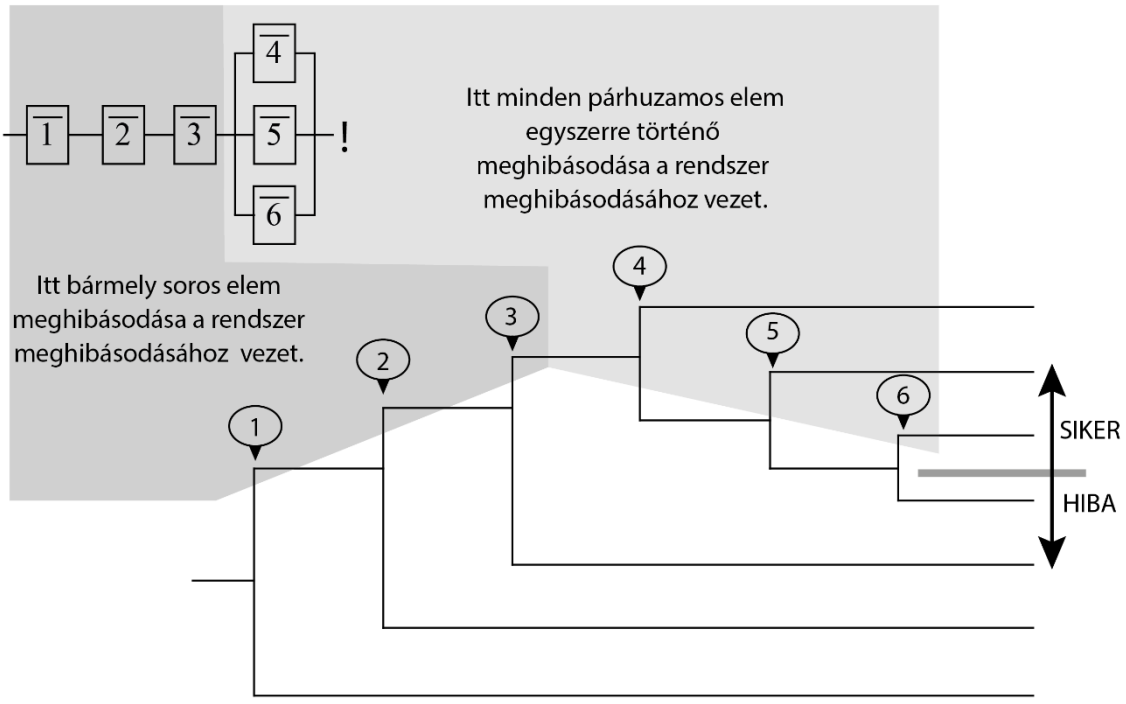
9.2 RBD és hibafa konverziója eseményfává

Ahogy láttuk az eseményfa elemzésénél, az eseményfa sikeres ágai a vágatok halmazaival, míg a meghibásodásokat reprezentáló ágai a path halmazokkal egyeznek meg. Így tehát ha ismerjük a vágatok halmazait és a path halmazokat egy adott csúcseseményre nézve, képesek vagyunk az eseményfát ezekből elkészíteni. A cut és path halmazokat pedig generálhatjuk egy RBD-ből, ahogy a 9.2. ábra mutatja egyszerű esetben.



9.2. ábra. RBD-ből cut és path halmazok származtatása.

Az RBD-t közvetlenül eseményfává is tudjuk transzformálni, ahogy az alábbi ábrán látható.

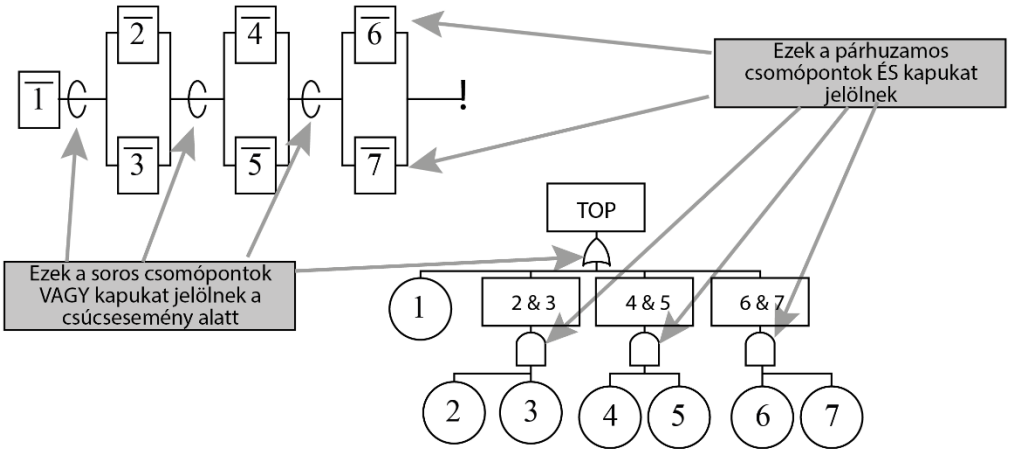


9.3. ábra. RBD - ETA konverzió.

9.3 RBD - hibafa konverzió

A hibafa azokat a rendszerfüggvényeket reprezentálja, melyek ha meghibásodnak, a csúcseseményt siker helyett hibára viszik, melybe a megbízhatósági blokk diagram valamely útvonala vezet. Soros csomópontok RBD-ben egy VAGY kaput jelölnek a csúcsesemény alatt a hibafában, a párhuzamos

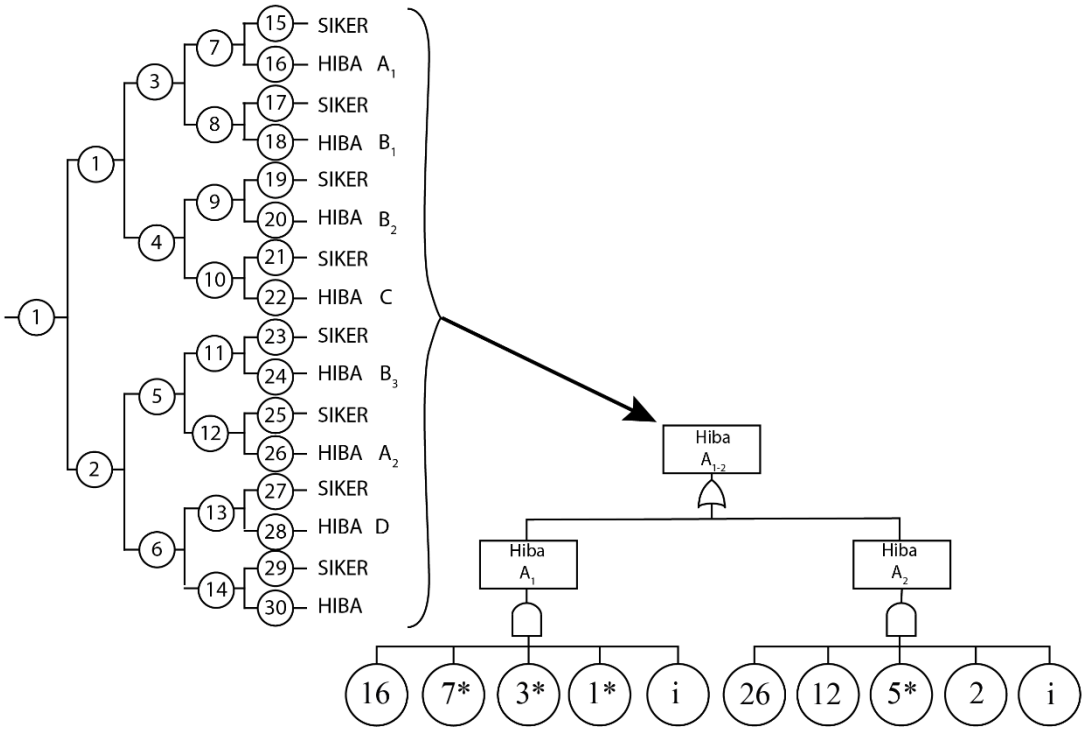
útvonalak pedig ÉS kapuval összekapcsolt redundáns komponens függvényeket. Ezeket figyelembe véve, a 9.4 látható konverziót alkalmazhatjuk.



9.4. ábra. RBD - hibafa konverzió.

9.4 Eseményfából RBD és hibafa konverzió

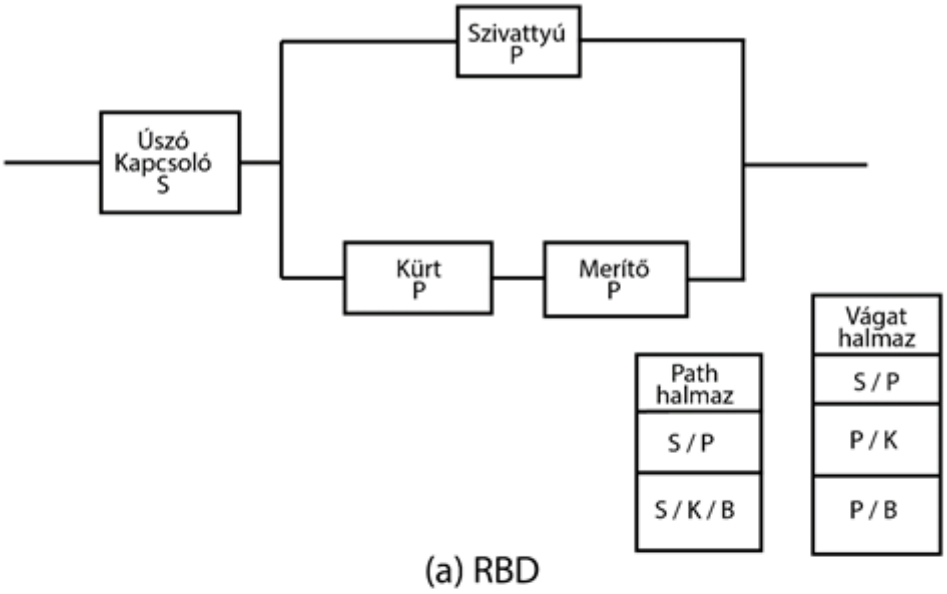
Az eseményfa path halmazokat reprezentál a sikeres útvonalain, és vágat halmazokat a meghibásodási útvonalain. Eseményfa RBD-vé konverziójához a 9.3. ábrán látható folyamat inverzét kell elvégeznünk. Ha az RBD elkészült, azt hibafává konvertálhatjuk az előző ábrán látható módon. Hasonlóan, egy eseményfa közvetlenül is hibafává alakítható, ahogy a következő ábra mutatja.



9.5. ábra. Eseményfa hibafává transzformálása.

9.5 Példa

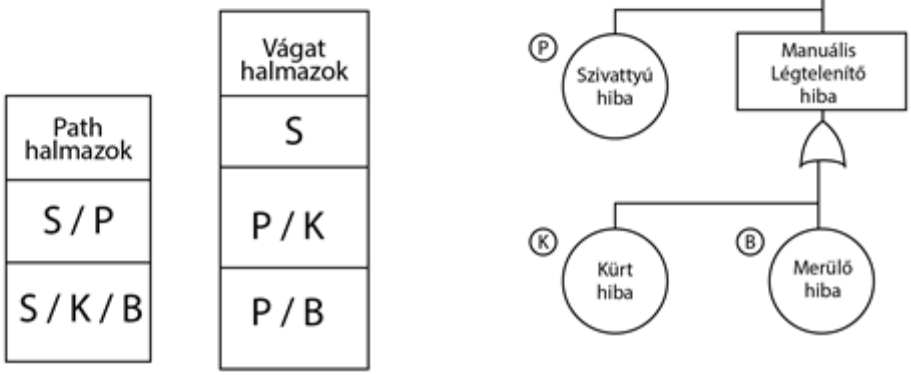
A fenti módszereket alkalmazva a 8.4. ábrán ismertetett eseményfára, az alábbi eredményeket kapjuk először RBD-vé, majd hibafává alakítva (9.6. ábra). Mindhárom modell a rendszer ekvivalens logikai reprezentációját adja.

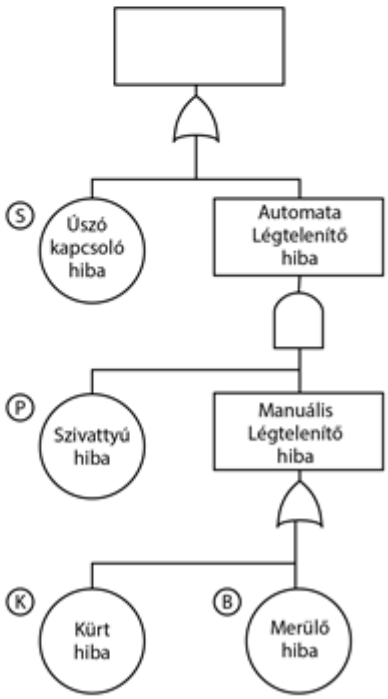


(a) RBD

$$P_{TOT} = P_S + P_P P_K - P_P P_K P_S + P_B P_P - P_B P_P P_S - P_B P_K P_P + P_B P_K P_P P_S$$

$$P_{TOT} = P_S + P_P P_K + P_P P_B$$





9.6. ábra. Az előző ábrán látható eseményfa transzformációi

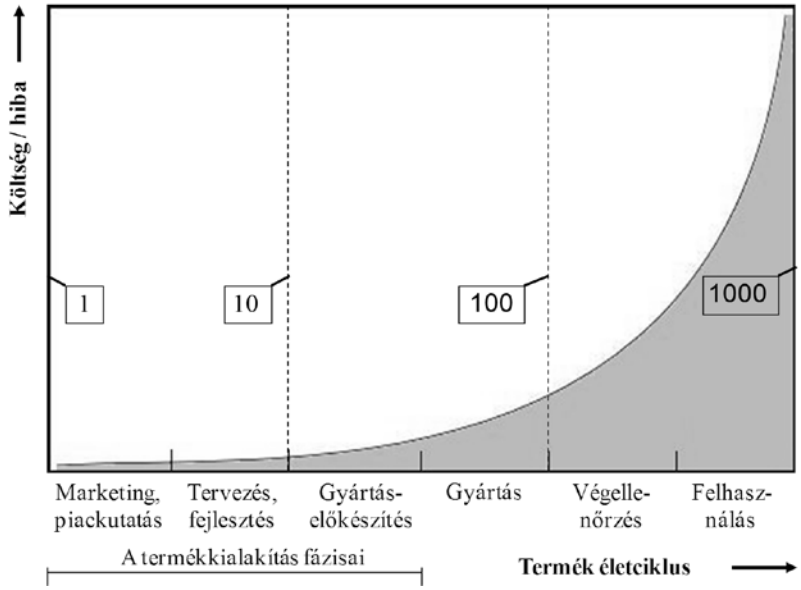
10 Tervezés biztonságra és megbízhatóságra

A megbízhatóságra való tervezés egy szisztematikus és multidiszciplináris megközelítés, amely a korai koncepció kialakítása során játszik alapvetően fontos szerepet. Cél, hogy jelentősen csökkentsük a potenciális hibaokok felbukkanását – amelyek kialakulásukkal hibaláncolathoz vezethetnek – és növeljük a termék hasznos élettartamát.

A megbízhatóság-menedzsment kölcsönös kapcsolat kialakítását segíti elő a termék életciklus-szakaszai és a termékhez kapcsolódó rendszer életciklus folyamatai között. A termék életciklus-szakaszait az ellátandó feladatokhoz (funkciókhoz) illesztik. A termék életciklus-szakaszai a következők: a termék koncepciójának kialakítása, tervezés és fejlesztés, gyártás, üzemeltetés, karbantartás és selejtezés. Ezekhez a szakaszokhoz kapcsolják és ezekbe a szakaszokba építik be a rendszer megbízhatósági programjának feladatait, amelyek felölelik többek között a beszerzést, a szállítást, a tervezést és szabályozást (ellenőrzést), az értékelést.

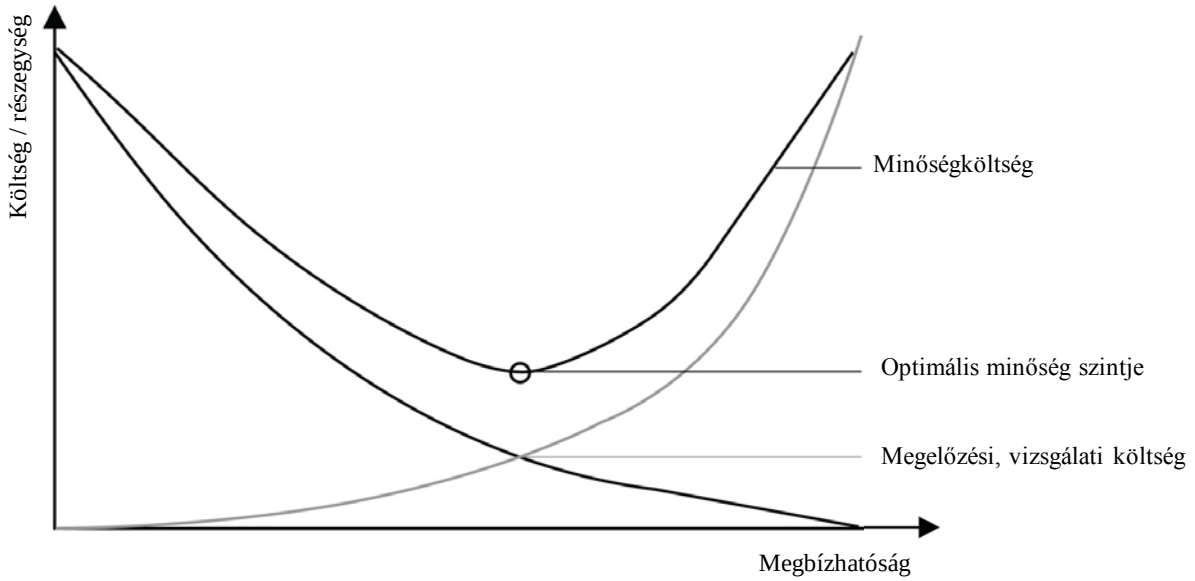
A koncepció fázisában végrehajtott vizsgálatok és alkalmazott módszerek csökkentik a műszaki kockázatot a termékfejlesztés során és jobb minőségű termék előállítását teszik lehetővé kevesebb tervezési, gyártási és kiegészítő költséggel. Előfordul, hogy programhibának titulálnak elégtelen analízist, de ez inkább a még szükséges és ajánlott elemzések kiválasztására és az olyan fogalmak tisztázására világít rá, mint a legrosszabb eset vizsgálata.

A vezetés által meghatározott elemzések mélysége mindig opcionális, amelyhez azonban előfordulhat, hogy a fejlesztőnek nem megfelelő eszközök állnak rendelkezésére, sőt, a végrehajtást sem feltétlenül ő végzi, hanem csupán támogató funkcióként jelenik meg a vizsgálat az elemzés során. A megbízhatósági vizsgálat felelősség, amelyet pontosan tisztázni kell és részt vesz benne a fejlesztő. Egy koncepció, amely nem felelt meg minden vizsgálatnak és tesztnek nem tekinthető megfelelőnek és nem hozható forgalomba. Bár bizonyos vizsgálatok (pl.: hő, hibamód és -hatás, logisztikai, gyárthatósági elemzés) további mérnökök bevonását igénylik, a végső kialakítás alacsonyan tartott költségét – egyre később felfedezett hibák esetén – többszörösen fizeti meg a gyártó (10.1. ábra).



10.1. ábra. Költség többszöröződése a hibák felfedezésének függvényében.

A hagyományos minőségköltség modell a megelőzési, vizsgálati költségre és a hibaköltségre terjed ki. A vizsgálati költségek magukba foglalnak teszteket, végellenőrzéseket, a megelőzési költségek olyan vizsgálatokra vonatkoznak, amelyek csökkentik a hibalehetőségeket minőségtervezéssel, ellenőrzéssel, audittal, tréninggel (10.2. ábra). Hibaköltségek akkor merülnek fel, ha a minőségi követelmények nem teljesülnek.



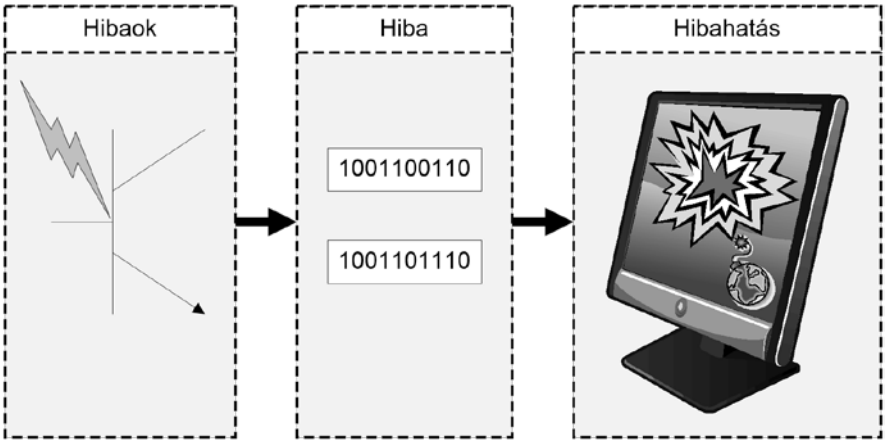
10.2. ábra. Optimális minőségi szint.

Egy nagy megbízhatóságú rendszer nem szükségszerűen hibatűrő. Olyan redundáns rendszer kívánatos, amely nagyszámú hibát képes tolerálni. Sok kritikus alkalmazás esetében a nagy megbízhatóság elérése érdekében a hibatűrés alapvető rendszertulajdonság. A redundáns rendszersémáknak két fő típusa van: tartalék és hibaelrejtő (két vagy több hibafeltétel kompenzálja egymást és a külső hiba nem jelenik meg mindaddig, amíg egyik elrejtést eredményező hiba kijavításra nem kerül). Érdekes, hogy az említett sémák esetén az eltűrt hibák száma igen alacsony

összehasonlítva az alkalmazott redundáns modulok számával. Ez magas költséget von maga után a megbízhatósági ráta eléréséhez.

A redundancia lényege, hogy egy funkcióhiba nem befolyásolja a rendszer működőképességét egy azzal megegyező back-up funkció aktiválásában. A redundancia kiépíthető mind hardver, mind szoftver vagy mindkét szinten, de manapság elfogadott tény, hogy a számítógépes rendszerek nem tudják elérni a kívánt megbízhatóságot és hibatűrést a szerkezetükbe épített redundancia nélkül. Különbséget kell tennünk aktív és passzív működésű megoldások között. Amíg az előbbi esetben szimultán működik a rendszer háttérben, az utóbbiban inaktív és csak akkor kapcsol be, ha az elsődleges eszköznél funkcióhiba lép fel.

Mivel az elektronikus rendszerek váratlanul, véletlenszerűen hibásodhatnak meg (10.3. ábra) minden figyelmeztetés és előjel nélkül, a biztonságkritikus funkciók biztosításához redundáns és hibatűrő rendszereket alkalmaznak, pl.: repülőipar. A redundancia nyilvánvaló előnye, hogy tartalék áll rendelkezésre hibás komponens esetén. A repülésben a safe-life (hibamentes) rendszereket írják elő elkerülendő a hiba megjelenése. Mint az közismert, a levegőben még nem maradt repülőgép, ezért biztosítani kell a folyamatos működést, ameddig a leszállás lehetővé nem válik.



10.3. ábra. Hibaok – hibahatás.

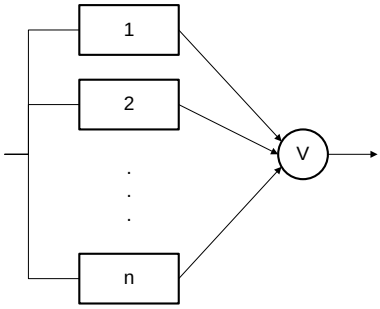
Az elemzések során el kell dönteni, mely biztonsági intézkedéseket fontos megvizsgálni. A célok között szerepel a visszaállítás, hibatűrés és üzembiztosság. A folyamat visszaállítható, ha a hibahatás megjelenése után a folyamat irányítása lehetséges és elfogható időn belül visszaállítható a normál működésbe. Egy folyamat hibatűrő, ha a hibahatás megjelenése ellenére, mégha csökkentett módban is, képes a funkcióját ellátni. Egy rendszer akkor üzembiztos, ha a hiba(kombinációk) megjelenésének ellenére nem kerül biztonságot veszélyeztető állapotba és leáll a működése, amikor elérte az energiaminimumot, pl.: a jármű megáll. Egyszeres hiba kritériuma esetén a rendszert úgy kell megalkotni, hogy egy hibaok ne okozhasson hibát. Az egyszeres hibát detektálni kell, ha

- a hiba detektálható,
- véges számú hiba lehetséges,
- az első után felbukkanhat a következő,
- azonban az első mégsem sikerül, a detektálható hibák tűrésére van szükség.

A by-wire rendszerek, mint pl.: kormány, váltó, motor sok előnnyel szolgálnak járművezetés közben, ezért egy átfogó rendszerbiztonsági folyamat, program kidolgozása szükséges, amely tartalmazza

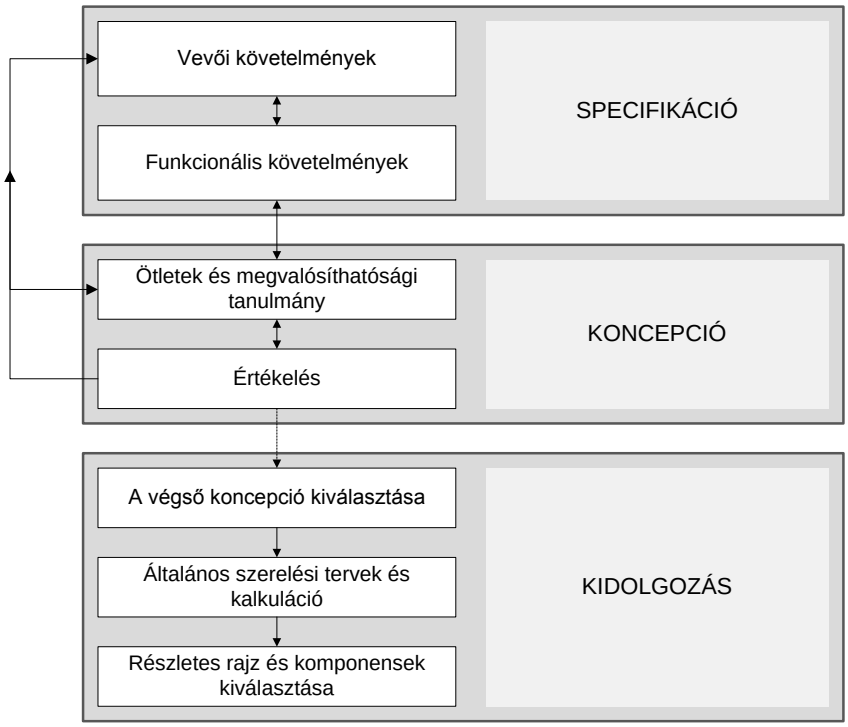
- a potenciális veszélyeket és az elkerülésükhöz betartandó követelményeket
- a biztonsági követelmények műszaki meghatározását
- a tervezés értékelésének menetét és támogatást az aktuális fejlesztéshez
- a követelmények kielégítésére vonatkozó értékelést
- a közvetlen és közvetett biztonsági vizsgálatokat
- a felülvizsgálati tevékenységeket és a biztonsági irányvonalat

Kritikus rendszerek esetén a megbízhatóság növelésére szívesen alkalmazzák az N számú modul redundancia (NMR) módszert (10.4. ábra). Az űrhajózásban a redundanciát illetően fokozott előkészületre van szükség, ahol nem ritka a többszörös, akár háromszoros, négyszeres tartalékrendszer használata sem.



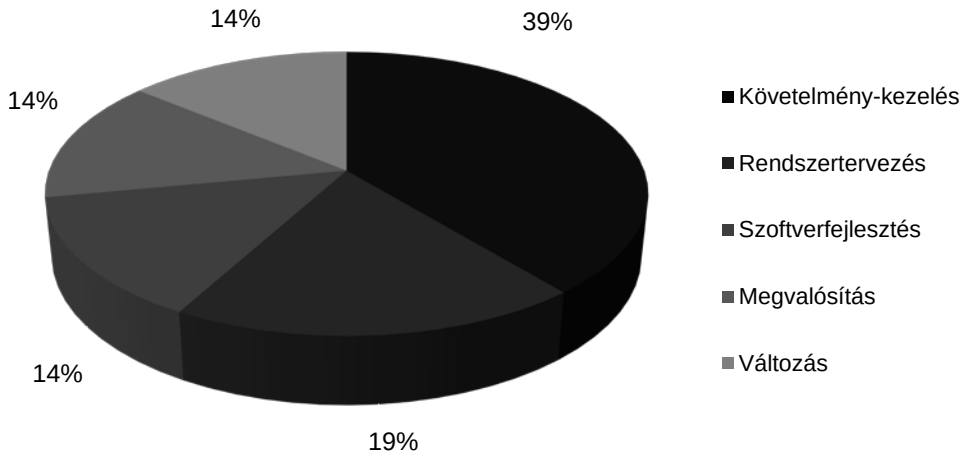
10.4. ábra. NMR rendszer.

A megbízhatóság és a fenntarthatóság alkalmazása alapvető bármilyen komplex termék vagy rendszer előállítása esetén. Ahhoz, hogy ezek az elvek hangsúlyosak maradjanak, a megfelelő egyensúly megtalálása szükséges a minden határon túli megbízhatóság és a versenyképesség között. Az egyre bonyolultabb elektronikus rendszerek miatt a megbízhatóság és gyárthatóság, a minőség és támogatás egyre fontosabb a műszaki tervezésben, ahol a jó koncepció mind inkább előtérbe kerül (10.5. ábra).



10.5. ábra. Iteráció a tervezésben.

Az asszisztens funkciók, mint járulékos szolgáltatások jellemzően ún. fail-safe stratégiával rendelkező elektronikus rendszerként működnek, amelyek kikapcsolnak, ha nem megfelelően látják el funkcióikat. A mechanikus back-up nélküli by-wire rendszerek az autóipari biztonsági követelmények új dimenzióját tárják fel, azaz a rendszernek detektált hiba esetén is szükséges a szolgáltatást nyújtania legalább egy előre meghatározott csökkentett módban [4].

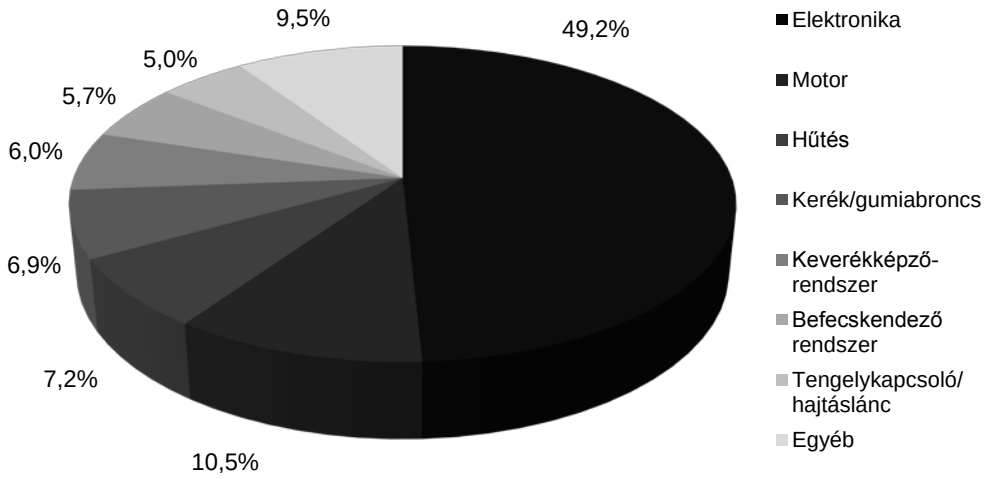


10.6. ábra. Vezető baleseti okok a tervezés során.

Jelenleg csak korlátozottan áll rendelkezésre statisztika a teherautók részvételével bekövetkezett balesetekkel kapcsolatban és még kevesebb adat, amely az okokat illeti. Az Európai Bizottság emiatt egy egyedülálló tudományos tanulmányt jelentett meg, amely ezzel a témakörrel foglalkozik (ETAC - European Truck Accident Causation) [5]. Mint ismeretes egy baleset bekövetkezésében több tényező együttesen játszik közre, amelyek egymásra hatással vannak, ezért a tanulmány célja beazonosítani a

leginkább szerepet játszó összetevőt. Kutatási szempontból a fő ok az, amely a legnagyobb mértékben idézte elő a baleset bekövetkezését (10.6. ábra).

A mai járműtervezésben számottevő százalékban jelennek meg elektronikai és kommunikációs rendszerek, illetve szoftvertechnológia a biztonságkritikus járműrendszerek területén még inkább növelve komplexitásukat [6] [7]. Manapság egy személygépkocsi költségének 30%-át teszi ki az elektronika és a gyártási költség 4%-át a szoftverek jelentik. Ez várhatóan 13%-ra növekszik majd és az új innovációk 90%-a elektronikus rendszereken alapul. A jelenlegi mikrokontrollerek átlagértéke 25db, de az évtized végére további növekedés várható. Becslések szerint a járműveken belüli hálózatok száma a mostani 5-ről 2015-re 15-re emelkedik. A rendszerkomplexitás növekedése biztonsági kérdéseket vet fel mind a járműre és az utasaira nézve is (10.7. ábra). A biztonságkritikus rendszerek körültekintő és szigorú tervezést kívánnak, illetve megfelelő tanúsító szerv által hagyhatóak jóvá.



10.7. ábra. Az autókban felmerülő főbb problémák.

A következőkben az alábbiakban ismertetett biztonsági stratégiák ismerhetők meg a haszonjárművek elektronikus fékrendszerein keresztül:

Fail silent – a rendszer amennyiben olyan hibát észlel, ami annak biztonságos működését veszélyezteti, a rendszer biztonságosan vagy részlegesen, vagy teljesen kikapcsol (egy jól meghatározott back-up funkcióba kerül), pl.:

- ABS – adott tengelyen detektált szenzorhiba esetén a tengelyt irányítását kikapcsolja, vezérlőegység elektronikus hibája esetén a teljes rendszer kikapcsol
- ESP – detektált szenzor plauzibilitási hiba esetén kikapcsol

A fail-silent rendszerek általában nem befolyásolják a rendszer alapfunkcionalitását (jármű fékezhetősége), emiatt nincs hardware back-up rendszerük.

Fail-safe – hibabiztos a rendszer és amennyiben olyan hibát észlel, ami annak biztonságos működését veszélyezteti, a rendszer egy jól meghatározott és biztonságosan működő, az alapfunkcionalitást a törvényi előírásoknak megfelelő módon biztosító back-up módba kerül, pl.:

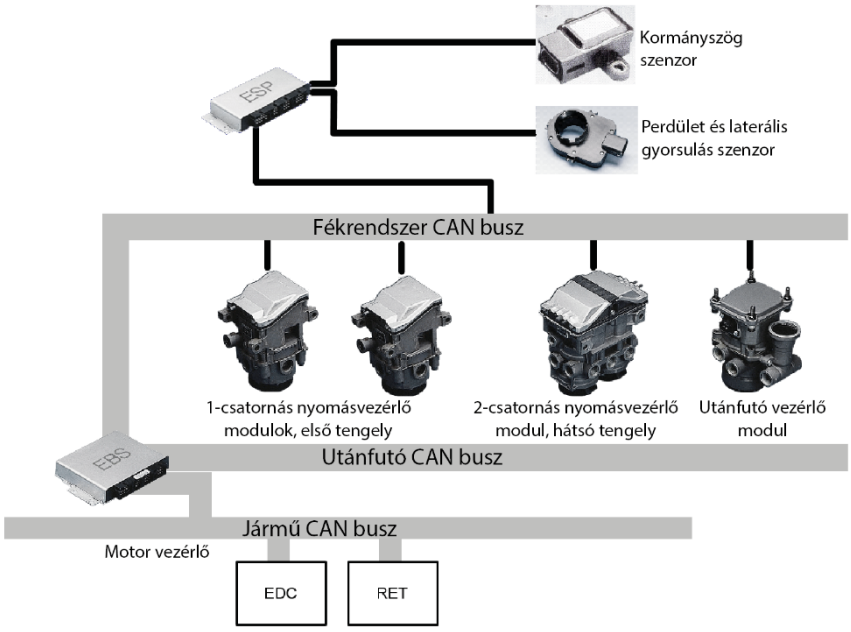
- EBS – adott tengelyen/modulon/szenzoron detektált hiba esetén vagy részlegesen (tehát az adott tengelyt kikapcsolva) vagy teljesen back-up módba kerül. A back-up ebben az esetben mindenképpen hardware redundanciát jelent.

A fail-safe követelmény az alapfunkcionalitást biztosító rendszerek esetében áll fenn, amikor az elsődleges rendszer teljes vagy részleges működésképtelensége esetén egy másik rendszer biztosítja a szükséges előírt funkcionalitást.

Fault-tolerant – hibatűrő a rendszer és funkcionalitása abban az esetben is teljes mértékben biztosított, ha az elsődleges rendszer meghibásodott, pl.:

- A rendszerrel szemben támasztott követelmény, hogy a „platooning” (járművek konjovban való haladása) üzemmód alatt az elsődleges rendszer kiesése után a második teljes mértékben biztosítja a teljes megkívánt funkcionalitást.

A következő képen a tehergépjárművekben 1996 óta Európában alkalmazott fékrendszerek tipikus felépítése látható (10.8. ábra).



10.8. ábra. Jellegzetes fékrendszer-felépítés.

A rendszer fő komponense az elektronikus fékrendszer elektronikus vezérlőegysége (EBS ECU), amely CAN (Controller Area Network) összeköttetéssel kommunikál a jármű egészével, a vontató járművel és egy saját fék CAN-nel. A kerék/tengely fékvezérlő modulok a fék CAN-hez csatlakoznak és az irányításuk ezen a buszon keresztül valósul meg. Rendszertől függően a vezérlő szoftver szétosztott a központi és a modul vezérlőegységek között. Az elektronikus stabilizáló rendszer esetében lehet külön vezérlőegység a fék CAN-hez csatlakoztatva vagy a funkció a központi vezérlőegység része és egy külön CAN busz biztosítja az összeköttetést a szenzorokkal.

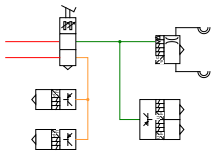
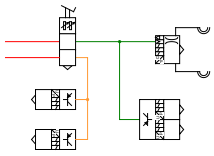
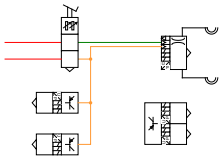
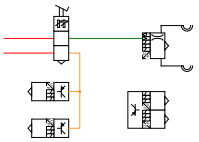
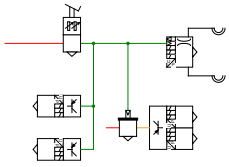
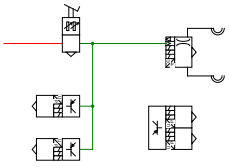
Ami a redundancia szintjét illeti, ezek a rendszerek egy elektronikus körrel rendelkeznek (ez vezérel minden modulátort) és – mint alapvető vevői elvárás – két pneumatikus rendszerrel, amelyek back-up rendszerként (vészrendszerként) funkcionálnak. Egyszeres hiba esetén az elektronikus körben a

felbukkanó hiba súlyosságától függően, a rendszer visszakapcsol egy részleges vagy teljes back-up módba, amely az alap fékfunkciót tekintve teljes redundanciával bír. Ez a felépítés kielégíti a törvényi követelményeket, de egy teljes pneumatikus vészrendszer működésbe lépése esetén számos funkció nem elérhető. Az ilyen rendszert hívjuk 1E+2P rendszernek (egy elektronikus és két pneumatikus kör).

Ráfordítási és konstrukciós megszorítások miatt folyamatos vita van arról, elhagyható-e a két pneumatikus kör egyike, ugyanis a törvényi előírásokat egy pneumatikus kör megléte esetén is kielégíti. Ez azt jelenti, hogy a pneumatikus vészrendszer nem szükséges sem a tréler vezérlőszelepénél (TCM), sem a hátsó tengely esetében.

Az alábbi táblázat (10.1. táblázat) a leginkább jellemző fékrendszer elrendezéseket és redundancia szinteket mutatja két körös pneumatikus lábfék szeleppel 1E+2P rendszer esetén (de a hátsó tengelyen és a tréler vezérlőszelepben lévő vészrendszer nélkül), illetve azokat az 1E+1P rendszereket, ahol a lábfék modul (FBM) csak egy körrel rendelkezik.

10.1. táblázat. Lehetséges fékrendszer architektúrák vészrendszereik függvényében.

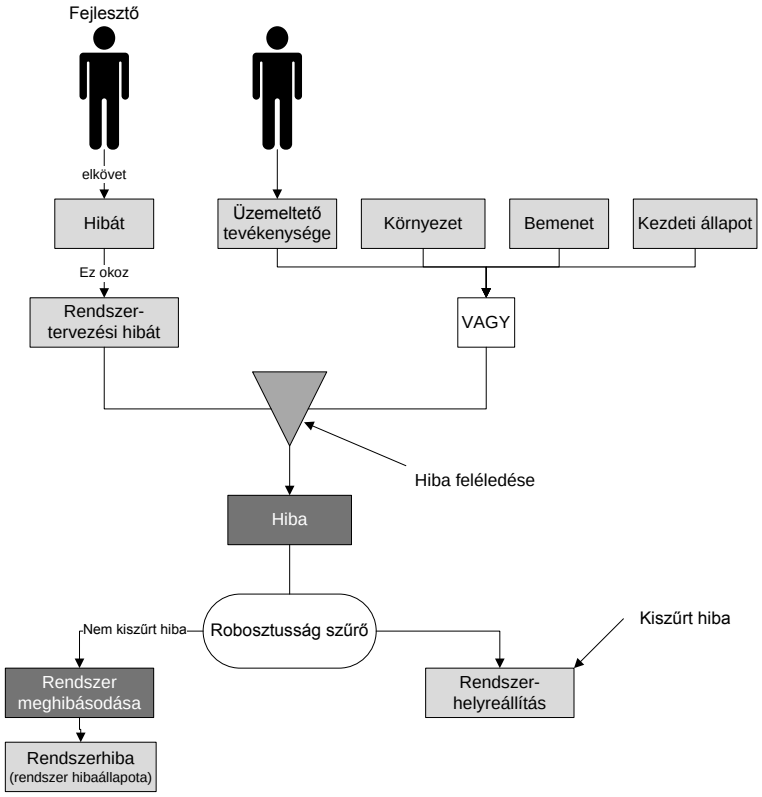
	Hátsó tengely vészrendszerrel		**Hátsó tengely vészrendszer nélkül**	
	TCM 2P-vel	TCM 1P-vel	TCM 2P-vel	TCM 1P-vel
FBM 2P+1E				
FBM 1P+1E				

A két 1E+1P elrendezés kielégíti a törvényi előírásokat megtartva az alap fékrendszer fail-safe (hibabiztos) tulajdonságát, amely azt jelenti, hogy egyszeres hiba esetén is teljesíti az előírt csökkentett módú működést, bár az elektronikus kör hibája esetén, sem az ABS, sem a fékerőelosztás stb. funkció nem érhető el. Az 1E+1P architektúra azonban nem illeszkedik az autonóm vezetés követelményeihez, mert a külső fékigény átvitele nem lehetséges pneumatikus vészrendszer módban. Ez azt jelenti, hogy ebből a szempontból a rendszer sem hibatűrő, sem hibabiztos.

11 Emberi tényezők

11.1 Emberi tényezők megbízhatósági kérdései

A rendszer megbízhatósága szempontjából lényeges az emberi beavatkozás hatása, ugyanakkor alkatrész-megbízhatóság szempontjából kevésbé fontos. Az emberi tényező megbízhatóságát nem szabad az ember hibamentes tevékenységére korlátozni (11.1. ábra) [8].



11.1. ábra. Hibalánc a tervezési fázisban.

Az emberi beavatkozás hatásait két szempontból kell vizsgálni:

- Azok az emberi beavatkozások, amelyek nem az üzemeltetés során éreztetik hatásukat. Ilyen tevékenységet végeznek a tervező mérnökök és a menedzserek.
- Azok az emberi beavatkozások, amelyek közvetlenül befolyásolják a rendszer működését a rendszer üzemeltetése és karbantartása során.

Az emberi beavatkozások részletesebb csoportosítása a következő:

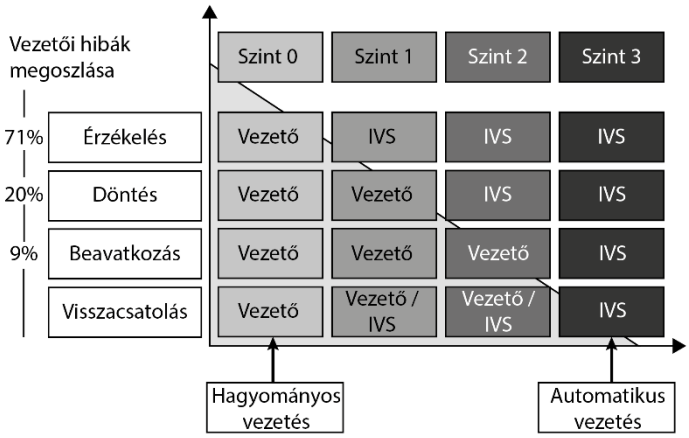
- Beavatkozás a rendszer ember-gép kapcsolat során
- Beavatkozás a hálózaton keresztül (például egy másik rendszer ember-gép kapcsolatából kezdeményezték)
- Beavatkozás, amely fizikailag a környezetből történik, eltérően az ember-gép kapcsolatból származó beavatkozásoktól

Az ember-gép kapcsolatra a következő megbízhatósági követelmények vannak:

- Védelem a rendszer illegális elérése és az illegális belépés ellen
- Világosan érthető felhasználási utasítások

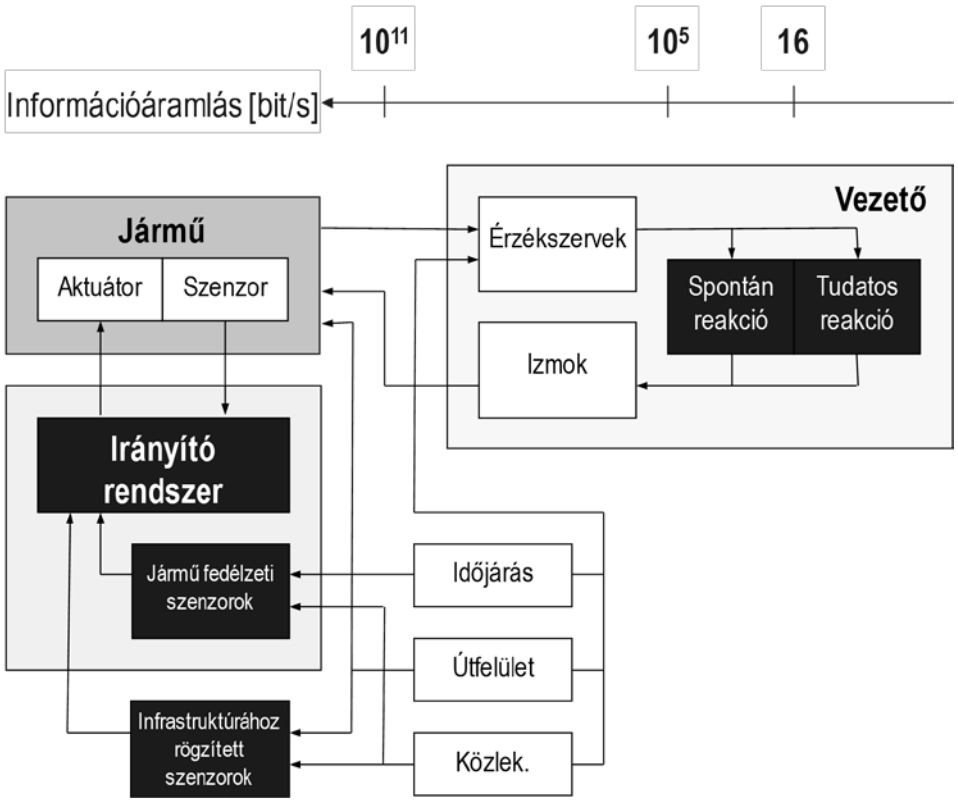
- Könnyen megvalósítható, magas szintű interaktív kapcsolat az ember és a gép között (könnyű kezelhetőség, üzembiztonság, a hibás bemeneti jelek megakadályozása, rövid idő alatti helyreállítás emberi hibák esetén)

A közlekedési balesetek elemzései azt mutatják, hogy az esetek 90%-ában a jármű vezetője (driver) a baleset elsődleges okozója. Ha jobban megnézzük a vizsgálatok eredményeit, láthatjuk, hogy 71%-ban érzékelési, 20%-ban döntési, 9%-ban beavatkozásbeli hibáról (driver failure rate) beszélhetünk. Ezek az értékek alapozzák meg az intelligens járműrendszerek használatát és fejlesztését, amelyek ellensúlyozzák a járművezető hiányosságait.



11.2. ábra. Az intelligens járműrendszerek osztályozása.

A fenti kép (11.2. ábra) az intelligens járműrendszerek (IVS – Intelligent Vehicle System) besorolását mutatja beavatkozásuk függvényében az érzékelés-döntés-beavatkozás-visszacsatolás (sensing-decision-action-feedback) folyamatában. Különböző szabályozási szintektől (level 0-4) függően (0: hagyományos irányítás [illegible] vitás), különböző rendszerek beavatkozására van szükség. Az első szint esetén, ahol az intelligens járműrendszerek csak érzékelik és tájékoztatják a vezetőt, nincs szükség hibatűrésre, elég, ha a rendszer fail-silent módban működik, azaz kikapcsol, ha kritikus hibát észlel. A harmadik szint esetében, amennyiben ténylegesen autonóm rendszer működéséről van szó, teljesen hibatűrő rendszert kell alkalmazni biztosítva a teljes funkcionalitást már egy kritikus hiba detektálásakor is. Természetesen ez lehet a vezető maga is, amennyiben biztonságosan át tudja venni az irányítást és a beavatkozó egységek hibátlanul működnek. A fenti probléma, bár új keletű a közúti járműiparban, nem számít újdonságnak a repülőgépiparban, illetve nagysebességű vasút esetében is találkozhatunk effajta technológiával.



11.3. ábra. Intelligens rendszerek beavatkozási hatásossága.

A járműről, annak környezetéből nagy sebességgel áramlik az információ a vezetőhöz, amíg azonban abból valamilyen tudatos reakció lesz, túl sok idő telik el. Ehhez hozzáadódik még az izmok reakcióideje, amelyek függnek a vezető pillanatnyi állapotától, valamint az a tény, hogy nem is mindenről rendelkezik információval. Ezek együttesen eredményezik az adott helyzetben való nem megfelelő reakciót.

Az intelligens járműrendszerek ezt a szabályozó kört nyitják fel, és akár a járműről, akár a jármű környezetéről gyűjtött információ alapján figyelmeztetést küldhetnek a vezetőnek (11.3. ábra). Be is avatkozhatnak azonban a jármű viselkedésébe akár úgy, hogy a vezető szándékát támogatják, de úgy is, hogy a vezetőt bizonyos időre felülbírálják és annak szándékával ellentétes beavatkozást fejtenek ki. Itt már érezhető az intelligens rendszerek alkalmazásának egyik központi problémája, hogy valóban ki lehet-e hagyni a vezetőt az irányítási hurokból. Ennek a kérdésnek a megválaszolása ma már kevésbe műszaki, sokkal inkább jogi és erkölcsi kérdés.

11.2 Betekintés a szoftverek megbízhatósági kérdéseibe

A korszerű rendszerekben a tervezés és az üzemeltetés során döntő jelentőségű szerepe van a szoftvernek. A szoftver ezért egyre lényegesebb a megbízhatóság szempontjából is (11.4. ábra). A rendszer megbízhatóságát nagymértékben befolyásolja az összes alkotóeleme közötti kölcsönhatás, ezért nem szabad a szoftver megbízhatóságát elkülönítve elemezni, vizsgálni és értékelni. Különösen távközlési berendezésekben meghatározóak a szoftverek.

A szakirodalom forrásaiból az alábbi következtetések vonhatóak le a szoftverek megbízhatósági vizsgálataival kapcsolatban:

- a hibamód- és hatáselemzés (FMEA) jelenleg adaptálódik, leginkább diagramok vagy leírások formájában léteznek,

- a szoftvereket fekete dobozként veszik figyelembe, amelynek megbízhatósága sosem ismerhető biztosan, csak becsülhető próbák után,
- a szoftver FMEA rendszerre való alkalmazása elég kevéssé publikált,
- a szoftver FMEA nem a szoftver megbízhatóságáról ad információt, hanem a felmerülő hiba hatását célozza meghatározni.

A megbízhatatlanság forrásai lehetnek az alábbiak:

- követelmények elemzése, értelmezése
- interfészspecifikáció (a rendszer alkotóelemeinek nem megfelelő specifikációja)
- hardverhibák
- szoftverhibák (a szoftver egy változója által felvett nem kívánt érték)

11.4. ábra. Elsősorban teszteléssel, hardverrel való integrálás során a kompatibilitást vizsgálják.

A szoftver megbízhatóság annak a valószínűsége, hogy a program egy adott időszak alatt nem okoz rendszer-meghibásodást a jelenlegi munkafeltételek mellett [9].

Szoftver megbízhatóság

- Nem jellemezhető a kádgörbével
- Nem öregszik el
- Viszonylag új terület
- Jól használható adatok gyűjtése nehéz
- A megbízhatóságot a tervezés befolyásolja
- Pénzt lehet vele megtakarítani
- A redundancia nem feltétlenül hatékony megoldás
- Klasszikus megbízhatósági vizsgálatok nehezen alkalmazhatók

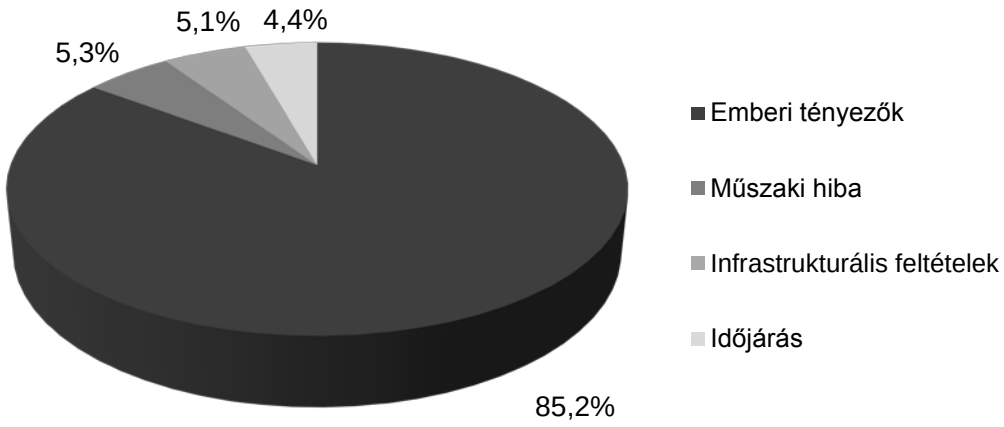
Hardver megbízhatóság

- Kádgörbével jellemezhető
- Elöregedés
- Jól megalapozott terület (főleg az elektronikus komponensek esetén)
- Jól használható adatok gyűjtése nehéz
- A megbízhatóságot befolyásolja mind a tervezés, a gyártás, a működés
- Pénzt lehet vele megtakarítani
- Általában a redundancia hatékony megoldás
- Klasszikus megbízhatósági vizsgálatok alkalmazhatók

A fejlesztés alatt folyamatos igény merül a termék megbízhatóságára vonatkozóan. Hangsúlyozni kell, hogy a szoftver domináns hibaokozó tényező a komplex rendszerekben. A szoftver MTBF értéke mutatja, hogy a hibákat megtalálták és eltávolították [10].

Az FMEA-t, ha használják is szoftver megbízhatóság elemzésre, leginkább olyan rendszerek esetén teszik, ahol minimális a hardvervédelem. A szoftverfejlesztés területén csak néhány szerző számolt be a megbízhatósági vizsgálat sikereiről [11].

A legtöbb hiba (11.5. ábra) a követelmény-menedzsment és a rendszertervezés fázisában keletkezik. A követelmény-menedzsment során keletkezett hibákat nem szűrik ki tesztekkel (a teszt ellenőrzést jelent, ha az implementáció a követelményeknek megfelelő). A specifikáció tiszta, pontos és egyértelmű kell, hogy legyen.



11.5. ábra. A szoftverhibákat kiváltó tényezők megoszlása.

A szoftverhibák értékelésére a hagyományos FMEA módszertant adaptálták és terjesztették ki az autóipari beágyazott valós idejű irányító rendszerek biztonságának vizsgálata során [12]. Az FMEA szoftverbiztonságra vonatkozó kiterjesztése lehetővé tette a potenciális hibák hatásainak átfogó elemzését beleértve az adatok sérülésének lehetőségét is. A szoftverre alkalmazott FMEA lehetővé teszi az egyszeres szoftverhiba és olyan hardverhibák értékelését, amelyek hatását a szoftver határozza meg.

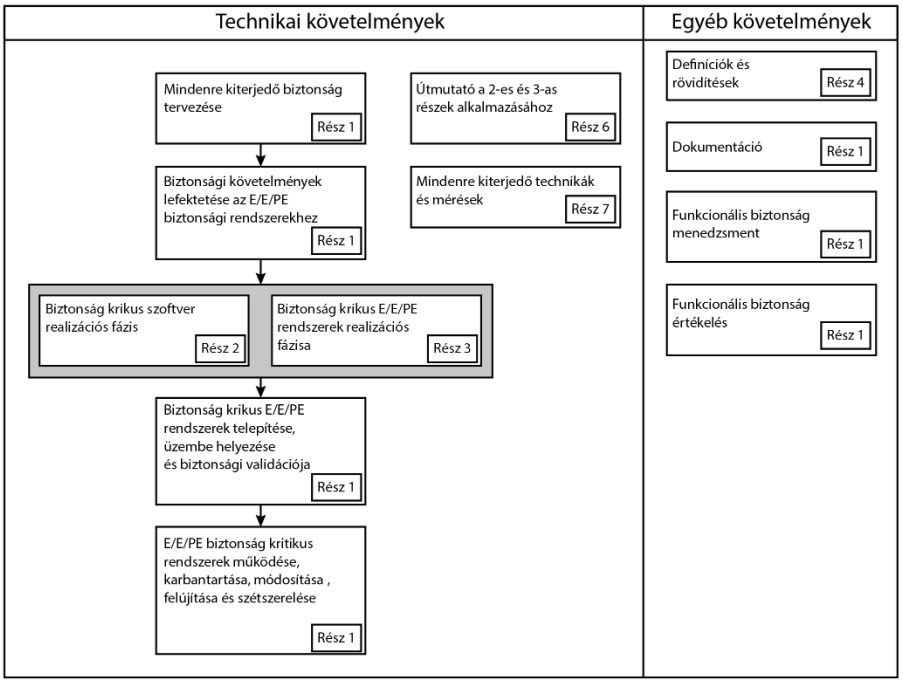
Az analitikus verifikációs technikák a hardverhibák értékelésére közismertek a megbízhatóság területén. Az FMEA és a FTA (hibafa-analízis) már bizonyított és sok a biztonságkritikus hardverrendszer értékelésére használt technika. Analitikus verifikációs módszerek léteznek ugyan szoftverre, de nem olyan ismertek a megbízhatóság területén, pl.: szoftver hibafa-analízis, Petri hálók.

A biztonságkritikus alkalmazások beágyazott irányítórendszerei olyan konstrukciót igényelnek, amely védelmet biztosít a hardver- és a szoftverhibáktól, illetve együttes megjelenésüktől. A rendszer sohasem kerülhet veszélyes, nem biztonságos üzemmódba. Azokban a rendszerekben, ahol hardverintegritási hibák léphetnek fel, a rávezető szoftver FMEA sokkal előnyösebb mint a szoftver hibafa-analízis.

12 Bevezetés a vonatkozó előírások követelményeibe

A biztonságkritikus (safety-related, safety-critical) elektromos/elektronikus/programozott elektronikus rendszerekre alkalmazott IEC 61508 szabványt a Nemzetközi Elektrotechnikai Bizottság fejlesztette ki (európai szervezet: CENELEC). Az ISO/IEC 61508 követelményeket határoz meg mind a tervezés, a fejlesztés, a működés és a biztonsági rendszerek irányításával, védelmével kapcsolatban, amelyek elektromos, elektronikus és szoftver technológiákon alapulnak. Egy rendszert biztonságkritikus rendszernek hívunk, ha megfelelő működés során fellépő bármilyen hiba veszélyt jelent az emberek számára (élet- és vagyonbiztonság), pl.: vasúti jelzések, járműirányítás, tűzveszélyesség stb.

A szabvány (12.1. ábra) lefedi az egész bizonsági életciklust, amelynek 16 fázisát a következőképpen lehet három részre osztani: 1-5 elemzés, 6-13 megvalósítás és 14-16 működés. A szabvány 7 részből áll: 1-3 szabványkövetelmények, 4-7 irányelvek és példák a fejlesztésre.



12.1. ábra. Az IEC 61508 felépítése.

1. rész: Általános követelmények
2. rész: Elektromos/elektronikus/programozható elektronikus biztonsági rendszerek
3. rész: Szoftverkövetelmények
4. rész: Definíciók és rövidítések
5. rész: Módszertani példák a biztonság integritási szintek (SIL) meghatározására
6. rész: Irányrelvek az IEC 61508-2 és IEC 61508-3 alkalmazására
7. rész: Technikák és intézkedések áttekintése

Az IEC61508 általános megközelítést biztosít minden biztonsági tevékenységhez, de a kitűzött célok eléréséhez körültekintően kell megválasztani az alkalmazott módszereket és eljárásokat.

12.1 Betekintés a repülésbiztonsági előírásokba

A repülésbiztonságot általánosan a repülési kockázattal fejezik ki, amely egy elemi kockázati (ER) érték alapján határozható meg, ahol ER=10-6. Ez azt jelenti, hogy egy katasztrofához vezető hiba egymillió repülőóránként következhet be. A valóságban a repülési kockázat függ a repülőgép típusától, a működési feltételektől, a repülőgépvezetőktől, amely nagyobb (jobb érték, tehát kisebb) mint a meghatározott szint, tehát 10-7…10-9. (A kockázati érték a Budapest-Párizs repülőutat tekintve kb. 1,5 ER, míg ugyanez Budapesten a belvárosból a repülőtérre 40-70 ER-nek tekinthető a forgalmi viszonyoktól függően).

Az 12.1. táblázat bemutatja egy adott rendszer elfogadott hibarátáját a redundanciaszint ismeretében. Ezek a célélértékként szerepelnek a feljesztési folyamatban és vagy megfelelő tervezéssel vagy elegendő számú redundancia beépítésével érhetőek el. A gyakorlatban a kritikus elemek redundacia szintje eléri a négy-ötszörös mértéket. A tervezés során azoban a következő tényezők – biztonság, működési költség, ár, hely, tömeg – figyelembe vétele, megfelelő súlyú szerepeltetése elengedhetetlen és részletes viszgálatot követelnek meg a tervező részéről.

12.1. táblázat. Rendszermeghibásodás a redundancia mértékétől függően.

	A redundancia foka		
	0	1	2
	Egyszeres	Kétszeres	Háromszoros
Katasztrofális	A = 10^{-9}	B	C
Veszélyes	B = 10^{-7}	C	D
Nagy	C = 10^{-5}	D	D
Csekély	D = 10^{-3}	D	D
Nincs hatás	E = na	E	E

A légi közlekedés és a repülőipar követelményeit nemzetközi (ICAO International Civil Aviation Organization – Nemzetközi Polgári Repülési Szervezet, JAA Joint Aviation Authority – Társult Légügyi Hatóságok) és nemzeti szervezetek (Polgári Légiközlekedési Hatóság, majd Nemzeti Közlekedési Hatóság) határozzák meg. A tervezés, gyártás, működés, fenntartás, javítás, különböző vizsgálati módszerek, oktatás, tanfolyam, személyzet stb. vonatkozó előírásait a légi alkalmassági és a kapcsolódó dokumentumok tartalmazzák. A legfontosabb ilyen irányú követelményeket az ICAO által kiadott függelékben és kézikönyvben találjuk. Mivel az ICAO fogalmaz meg javaslatokat, ezeket a követeményeket át kell ültetni a nemzeti törvénykezésbe [13].

Minden repülőipari terméknek rendelkenie kell tanúsítvánnyal, amelynek két fajtája van: típus és légi alkalmassági. A légi alkalmassági a fizikai és a törvényi megfelelőséget igazolja. Egy repülőgép (al)rendszerei és részei akkor felelnek meg a követelményeknek, ha fizikailag megfelelő állapotban vannak és rendelkeznek a fent említett kétféle jóváhagyással teljesítve a biztonsági előírásokat. A típusra vonatkozó jóváhagyás egy légügyi hatósági dokumentum, amely felhatalmazást ad egy adott repülőgép gyártására és üzemeltetésére. A légi alkalmassági tanúsítvány szintén egy légügyi hatósági dokumentum, amely egy adott repülőgép biztonságos üzemeltetésére ad felhatalmazást. A repülőgépváz gyártók olyan minőségmendzsment rendszert dolgoztak ki, amely kiterjed a beszállítókra is (pl.: fékrendszer):

- ISO 9001:2000
- Műszaki tervezési szabványok
- AIR 1934 (Speciális fékszerkezettel kapcsolatos előírások)
- AIR1064 (Fékdinamika)
- ARP1907 (Automata fékrendszer előírások)
- IEC 61508
- Légi közlekedési szabványok AMJ 25-1309 (berendezések és üzembe helyezés)
- SAE ARP 4754 (magas integráltsági szintű komplex repülőgép rendszerek tanúsításának vizsgálata)
- RTCA DO 254 (hardver tervezési útmutató) stb. [14]

12.2 A vasúti közlekedés biztonsági követelményeinek áttekintése

A biztonsági követelmények a vasúti közlekedésben mindig nagy hangsúllyal szerepelnek a rendszerfejlesztés során. Az előírások által szabályozott műszaki tervezés célja a RAMS (megbízhatóság, rendelkezésre állás, karbantarthatóság, biztonság) követeleményeit egy meghatározott szintig kielégíteni. A törvénykezés egyrészről nemzeti szinten jelenik meg, a mértékadó szabványok azonban mindinkább európaiak (CENELEC rendszer: EN 50126, EN 50129 és EN 50128), sőt nemzetköziek (IEC 61508). A CENELEC referencia rendszer célja:

- Közös szervezeti rendszer biztosítása Európában a vasúti komponensek piacának bővítésére, interoperabilitására, cserélhetőségére
- Vasúti sajátosságok azonosítása, új rendszerek komplexitásának, RAMS követelményeinek vizsgálata

Mivel a vasúti rendszerek is nagymértékben programozható berendezésekkel rendelkeznek, következésképpen fontos szerep jut a kapcsolódó szoftvereknek, amelyek szintén a RAMS előírásai alapján működtethetők és fejleszthetők megfelelő elemzési módszerekkel (FMECA, FTA etc.). Az EN 50128 szabvány kifejezetten a vasúti szoftverfejlesztéssel foglalkozik. Az itt meghatározott szoftver biztonsági integritási szint (SSIL) mind a négy szintjére, 0-tól (nem kritikus) 4-ig (kritikus) különböző fejlesztési tevékenységek kerültek meghatározásra (beleértve a verifikációt és a validációt).

A RAMS a rendszer hosszú távú működésének egyik sajátossága, amit a rendszer életciklusa során alkalmazott megalapozott mérnöki koncepciókkal, módszerekkel és eljárásokkal érnek el. Egy rendszer RAMS-a úgy jellemezhető, mint annak minőségi és mennyiségi fokmérője, hogy számítani lehet arra, hogy a rendszer, vagy a rendszert alkotó alrendszerek, illetve alkatelemek ellátják specifikált funkciójukat, ugyanakkor valamennyijük üzemkészsége és biztonsága megfelel a specifikációnak. A rendszer RAMS-a ezen európai szabvány vonatkozásában a megbízhatóság, üzemkészség, karbantarthatóság és biztonság kombinációját jelenti.

Egy vasúti rendszer célja, hogy meghatározott szintű vasúti forgalmat biztonságosan, adott idő alatt legyen képes lebonyolítani. A vasúti RAMS leírja azt a megbízhatóságot, amellyel egy vasúti rendszer e cél elérését szavatolni tudja. A vasúti RAMS egyértelműen befolyásolja a minőséget, amellyel a felhasználó számára nyújtja a szolgáltatást. A szolgáltatás minőségét egyéb, a funkcióval és a teljesítménnyel kapcsolatos jellemzők is befolyásolják, például a szolgáltatás gyakorisága, rendszeressége, és a díjszabási struktúra.

Az üzemkészség műszaki koncepciója a következők ismeretén alapul:

a) megbízhatóság szempontjából:
   - a meghatározott alkalmazásban és környezetben a rendszer összes meghibásodási módja,
   - bármely hiba előfordulásának valószínűsége, vagy előfordulásának gyakorisága,
   - a rendszer funkcionalitását befolyásoló hiba hatása.
b) karbantarthatóság szempontjából:
   - a tervezett karbantartási művelethez szükséges idő,
   - a hibák felismeréséhez, azonosításához és helyének behatárolásához szükséges idő,
   - a meghibásodott rendszer helyreállításához szükséges idő (nem tervezett karbantartás).

A biztonság műszaki koncepciója a következők ismeretén alapul:

a) a rendszer minden lehetséges veszélyes állapota bármely üzemi, karbantartási és környezeti feltétel esetén,
b) minden lehetséges veszélyes állapot jellemzője a következmények súlyossága szempontjából,
c) biztonsági vonatkozású meghibásodások szempontjából:
   - biztonsági vonatkozású meghibásodások szempontjából:
   - Valamennyi veszélyes helyzetet eredményező rendszer-meghibásodási állapot (biztonsági vonatkozású hibaállapotok). Ez a megbízhatóságot befolyásoló hibák egy részhalmaza.
   - Bármely biztonsági vonatkozású rendszer-meghibásodási állapot előfordulási valószínűsége
   - Az események, meghibásodások, üzemi állapotok, környezeti feltételek olyan sorrendje és/vagy egybeesése, amely balesetet eredményezhet (azaz valamely veszélyes helyzet balesetet eredményez)
   - Az adott alkalmazás kapcsán bármely esemény, meghibásodás, üzemi állapot, ill. környezeti feltétel előfordulási valószínűsége.
d) a rendszer biztonsági vonatkozású alkatelemeinek karbantarthatósága szempontjából:
   - veszéllyel vagy biztonsági vonatkozású hibaállapottal kapcsolatos rendszerelemek vagy alkatrészek karbantartásának egyszerűsége
   - a rendszer biztonsági vonatkozású elemein végzett karbantartás ideje alatt fellépő hibák valószínűsége
   - a rendszer biztonságos üzembe való visszaállításához szükséges időtartam
e) a rendszer biztonsági vonatkozású elemeinek üzemeltetése és karbantartása szempontjából:
   - az emberi tényezők hatása a rendszer valamennyi biztonsági vonatkozású alkatelemeinek hatékony karbantartására és a rendszer biztonságos üzemére,
   - a rendszer biztonsági vonatkozású elemeinek hatékony karbantartásához, illetve a biztonságos működéshez szükséges eszközök, berendezések és eljárások,
   - a veszélyeztetésekkel és azok következményeinek csökkentésével kapcsolatos hatékony intézkedések és hatékony felügyelet.

12.3 Autóipari követelmények áttekintése

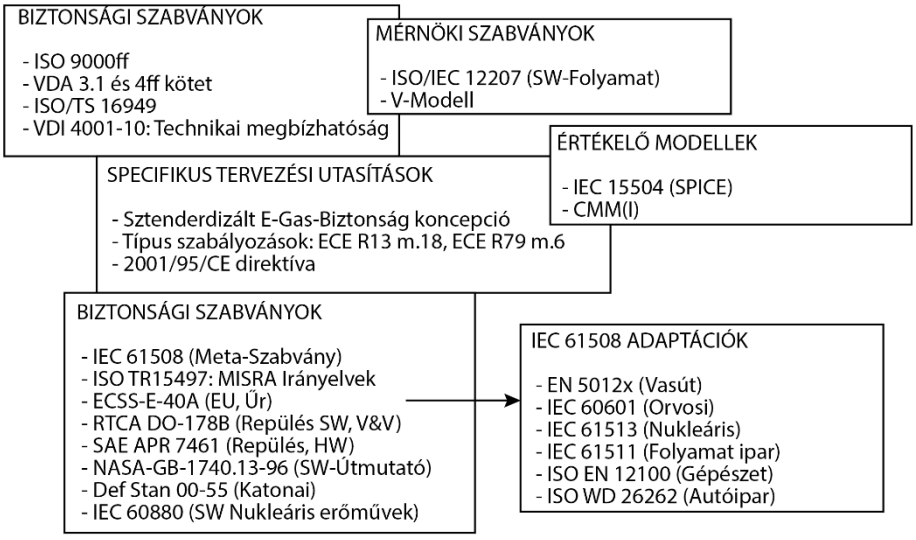
Az autóiparban szintén folyamatosan növekvő szerep jut a biztonság témakörének, amely magában foglalja a vezetés, a részegységek és a szerkezet, rendszerek biztonságát. Az utóbbi erőteljesen függ az egyes komponensek meghibásodási valószínűségétől és attól, hogy a rendszer hogyan képes a hiba kezelésére. Tágabb értelemben a rendszerbiztonság, megbízhatóság a rendszer katasztrofális hiba

nélküli biztonságos működését, emberre való veszélytelenségét, miközben a rendelkezésre állás és megbízhatóság a rendszer folyamatos működőképességét fejezi ki.

Az autóiparban jellemző új tervezési módszerek jobb minőségű és megbízhatóságú, gyorsabb és olcsóbb termékfejlesztést tesznek lehetővé. Az elmúlt pár évben a közlekedésbiztonság növelésére alkalmazott intelligens támogató rendszerek (blokkolásgátló fékrendszer, fékasszisztens, elektronikus menetstabilizátor stb.) mind működési, mind konstrukciós előnyökkel rendelkeznek, de alkalmazásuk biztonságkritikus rendszerekben a tervezési és fejlesztési folyamatok során különleges kezelést igényel.

Az autóiparban leginkább használt szabványok (12.2. ábra) mindinkább a korábban már említett IEC 61508 biztonsági szabványhoz hasonlóak. Egy Egyesült Királyságban (EK) működő autóipari konzorcium jelentette meg a MISRA irányelveket (járműipari szoftverek fejlesztési irányelvei). A MISRA konzorcium az EK motorgyártóit és az elektronikus egységek beszállítóit tömöríti és az említett irányelvek széles körben elterjedtek a nemzetközi autóelktronikai iparban. Olyan elveket és koncepciót tartalmaznak, mint pl.:

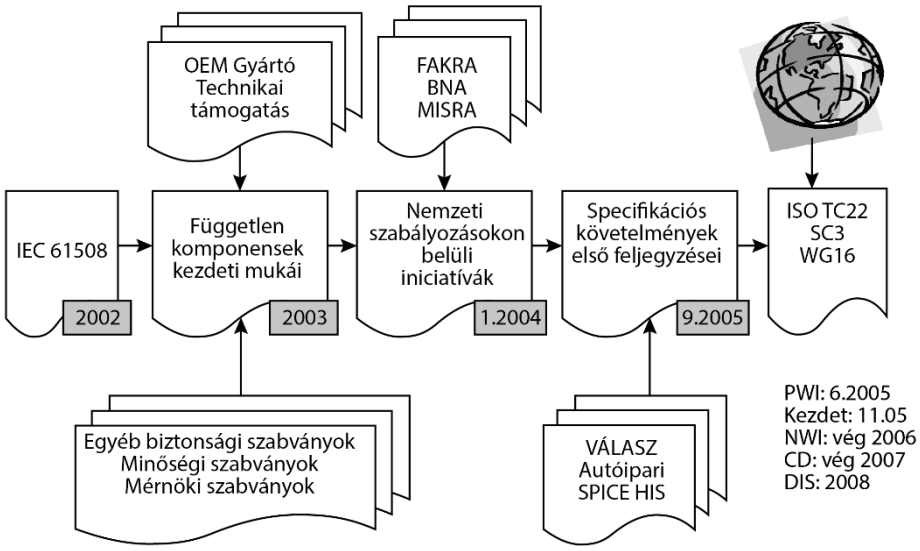
- A biztonság olyan, mint a demokrácia, látni kell, hogy létezzen
- Szoftver robusztusság, megbízhatóság és így a biztonság előnyt kell, hogy élvezzen
- A rendszertervezéskor figyelembe kell venni a mind a véletlenszerű, mind a szisztematikus hibákat
- A robusztusság megléte elengedhetetlen, nem bízhatunk a hibátlan működésben
- A biztonsági megfontolásokat a tervezés, a gyártás, a működés, a javítás és a szállítás során is alkalmazni kell



12.2. ábra. Szabványok és előírások áttekintése.

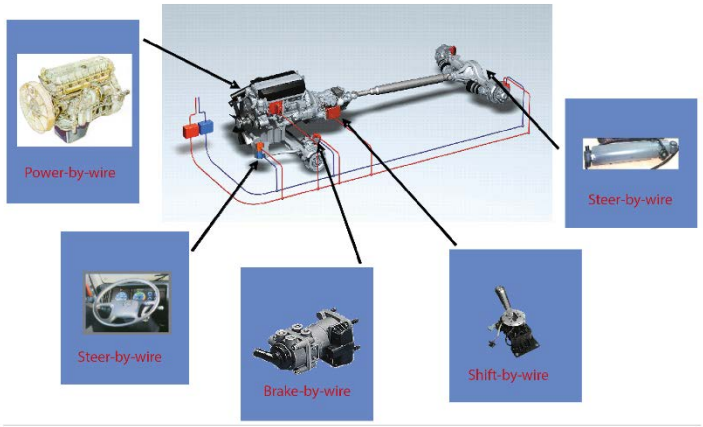
Ha a fenti elvárásokat a közúti balesetekben kárt szenvedettek oldaláról közelítjük meg, akkor kimutatható, hogy a haszongépjárművek részvételével bekövetkezett balesetek biztonságkritikus jellemzője legalább akkora, mint egy repülőgép szerencsétlenségé, csak az esemény gyakoribb bekövetkezésére való tekintettel kevésbé figyelemfelkeltő. A törvénykezés szereplői többek között ezért is gyakorolnak egyre nagyobb nyomást a gyártókra a termékek biztonsági szintjeit illetően. A

biztonságkritikus elektronikus rendszerek követelményeit az IEC 61508 tartalmazza, amelyek megjelennek néhány nemzeti szabályozásban is (pl.: Németország, FAKRA – Fachnormenausschuss Kraftfahrzeuge). Az ISO (Nemzetközi Szabványügyi Szervezet) által fejlesztett autóipari funkcionális biztonsági szabvány (ISO TC22/SC3/WG16) pedig az IEC 61508 előírásaival még szorosabban együttműködik (12.3. ábra).



12.3. ábra. Az IEC 61508 autóipari alkalmazása: ISO WD 26262 megjelenése.

A by-wire rendszerek (12.4. ábra) már régóta jelen vannak a repülőgépgyártásban (fly-by-wire), a járműgyártásban azonban csak az utóbbi időben terjedtek el. Kihívást jelent az ilyen rendszerek megjelenése mechanikus, pneumatikus vagy hidraulikus back-up rendszer nélkül figyelembe véve a szabályozási hátteret, amely kizárólag ilyen technológia használtatát egyelőre nem teszi lehetővé. A rendszereknek emellett együttesen kell kielégíteniük a költséghatékonyság és a nagy megbízhatóság követelményeit.



12.4. ábra. By-wire járműrendszerek.

A haszonjárművek fékrendszereire vonatkozó előírásokat az ENSZ-EGB (Egyesült Nemzetek Szervezete Európai Gazdasági Bizottsága) 13-as szabályozás foglalja magában. Szemelvények a legfontosabb követelményekből:

- kétkörös fékrendszer (a biztonsági fék a gyártó által meghatározott) – előírt lassulási értékek (min. 5 m/s2)
- egy hiba feltételezése (a hiba észrevehető!)
- ABS-szel felszerelt haszongépjármű
- kétoldalon eltérő (tapadású) útfelületen járműstabilitás biztosítása, megfelelő lassulás elérése
- rögzítő fék mechanikus kapcsolattal (meghatározott meredekség pókocsival vagy anélkül)
- tartós fék vagy a fékbetétek ellenállása az igénybevételnek (ciklikus fékezés – melegítés)
- az elektromos vezérlés átvitelében keletkezett elsődleges hiba (<40ms) ne legyen észrevehető hatással az üzemi fékrendszerre, tartós hibát jelezni kell (figyelmeztető jelzés)
- ha az akkumulátor feszültsége bizonyos (gyártó) érték alá csökken – vörös figyelmeztető jelzés
- kapcsolóponti szabályozás csak a vontató járművön lehet

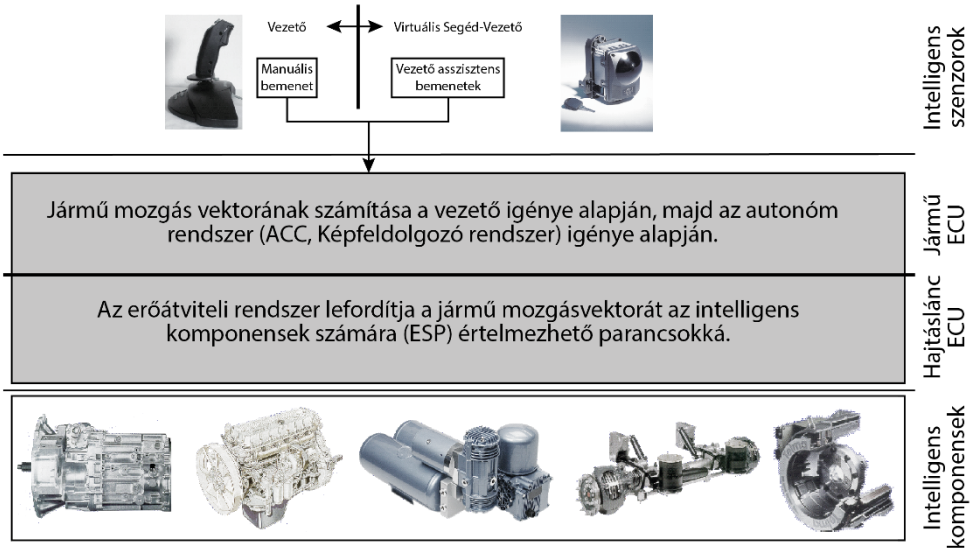
Egy repülőgép fékrendszere kifejezetten kritikus rendszernek tekinthető különös tekintettel egy leállított felszállási folyamatra, amely során az egész terhelt jármű lassítása és megállítása szükséges, illetve a leszállásra, amely hibás működés esetén irányíthatatlanságot okozhat. Ez magyarázza a repülőgép fékrendszerek jellemző felépítését. Mind az irányító-, mind az energiaellátó-rendszer redundáns és valamennyi meghatározó komponens megkettőzött. Egyszeres hiba esetén a rendszer működőképes marad és egy második hiba esetén is lehetőség van a csökkentett funkcionalitás biztosítására. A fizikai redundancia mellett további humán támogatás is része a rendszernek, mivel a repülőgép vezetője felülbírálható rossz döntés vagy alkalmatlanság esetén.

Egy autó és egy repülőgép fékrendszerének elvi működésében nincs nagy különbség, kivéve az elnyelendő energia nagyságát és a repülőgép fékek hűtésére rendelkezésre álló időt. Az előbb említett speciális jellemző magyarázza a repülőgépek jellegzetes felépítését számos álló és forgó tárcsával (a felhasznált kompozit anyagok nagyobb hőellenállással rendelkeznek). A kisebb repülőgépek fékrendszereinek működési környezete inkább hasonlít egy autóéhoz, amelynek piaca gyorsabban is növekszik mint a kereskedelmi és katonai repülésé.

12.2. táblázat. Összehasonlítás az iparági jellemzők alapján.

Repülőgépipar	**Autóipar**
Hosszú életciklus	Rövid életciklus
Hosszú piacra jutási idő	Rövid piacra jutási idő
Kis darabszámú termék	Nagy darabszámú termék
Szigorú biztonsági megbízhatósági hatósági előírások	
Közvetlen kapcsolat az emberrel	
Magas komplexitású rendszerek	
A berendezések több mint 30%-a E/E/EP	
Magas innovációs igény	
A vásárló nagy működési megbízhatóságot követel meg	

Fő különbséget a tervezési céloknál, a működés körülményeinél és a fejlesztési folyamatban találunk, amely együttműködő fejlesztéssel, hosszú életciklussal és piacra jutási idővel jellemezhető (12.2. táblázat). Ha párhuzamot szeretnénk húzni a repülőgép biztonságkritikus rendszereivel, egy igen hasonló rendszert határozhatunk meg (12.5. ábra).



12.5. ábra. A repülőgépirányítási rendszerrel analóg járműirányítási rendszer.

Ahogy a fenti képen látható, a kétszintű szerkezet mind logikailag, mind fizikailag szétválasztott:

- Irányítási szint (amely gyakorlatban a vezetői interfészt jelenti a gépjárműben): összegyűjt minden információt a jármű irányáról és környezetéről meghatározva az ún. célul kitűzött mozgásvektort
- Végrehajtási szint (hajtáslánc aktuátorokkal és szenzorokkal): irányítja a kölönálló aktuátorokat és megvalósítja a kívánt mozgásvektort

A mozgásvektor meghatározásakor a képen látható rendszer működése hasonló a két repülőgépvezető együttműködéséhez. Téves észlelés vagy hiba esetén a másik pilótának módja van a beavatkozásra. Az analógia itt nem egy más(od)ik személy, hanem szenzorok együttműködésével valósul meg összegyűjtve a környezetből származó információkat (radar- és videoszenzor, útviszonyok, időjárás stb.), ahol a vezető maga a „másodpilóta”. Ahhoz, hogy az autonóm járműirányítás biztonságosan megvalósuljon, az irányítási szint információi redundáns módon jutnak el a végrehajtási szintre, amelynek kommunikációs és energiaellátási rendszere is hasonlóan biztosított.

Ellenőrző kérdések

1. Definiálja a kockázat, a rendszer biztonsági mérnökség és a biztonság fogalmait, valamint adja meg a kockázati mátrix jelentőségét és használatának módját!
2. Írja le, hogy mi a SIL érték és mi az ASIL!
3. Adja meg a megbízhatóság és megbízhatósági ráta jelentését
4. Rajzolja fel a kádgörbét és értelmezze a szakaszatit
5. Adja meg az MTTFF, MTTF, MTBF, MTTR jelentését és jelentőségét a rendszer elérhetőségével kapcsolatban!
6. Milyen eljárást ismer összetett rendszer elérhetőségének számítására?
7. Mi az FMEA és hogy milyen FMEA típusokat ismer, azokat mire alkalmazzák?
8. Rajzoljon fel egy öt elemből álló hibafát és a hibafa alapján készítsen megbízhatósági blokk diagramot és eseményfát.
9. Mit jelent az, hogy 1oo2? Mire jó? Mivel jobb mint az 1oo1? Esetleg tudja számszerűsíteni?
10. Ismertesse a kockázatelemzés kvalitatív módszereit.
11. Milyen biztonsági stratégiákat ismer?
12. Mit jelent a fault-tolerant rendszerállapot?
13. Írjon két példát a fail-safe állapotra!
14. Miért és hogyan alkalmasabbak az intelligens rendszerek beavatkozásukat tekintve?
15. Milyen vezető-támogató rendszereket ismer?
16. Milyen közös szintek sorolhatóak fel a repülők és a haszonjárművek irányítási rendszerében és piaci jellemzőik tekintetében?
17. Soroljon legalább öt szabályozási szempontot (milyen rendszerre és hogyan terjed ki) az ENSZ-EGB 13-as előírásait illetően!
18. Mit jelent és mit jellemez a RAMS?
19. Hasonlítsa össze a hardver és szoftver redundancia sajátosságait!

Irodalomjegyzék

[1] P. Clemens, *Fault tree analysis, Fourth edition, Lecture presentation,* Sverdrup Technology, 1993.

[2] B. Goldberg, K. Everhart, R. Stevans, N. Babitt III, P. Clemens és L. Stout, *System engineering "toolbox" for design-oriented engineers,* National Technical Information Service, 1994.

[3] P. Clemens, *Event tree analysis. Second edition, Lecture presentation,* Sverdrup Technology, 2002.

[4] B. Hedenetz és A. V. Schedl, „Fault Injection and Fault Modeling for a Safety-critical Automotive Communication System," in *Safety and Reliability*, Rotterdam, Lydersen, Hansen & Sandtorv (eds), 1998, pp. 417-423.

[5] I. R. T. U. (IRU), *A Scientific Study 'ETAC' European Truck Accident Causation, Executive Summary and Recommendations,* 2007.

[6] J. R. Pimentel, „Verification, validation and certification issues of safety-critical communication systems," in *Safety-critical automotive systems*, Society of Automotive Engineers, Inc., 2006, pp. 3-12.

[7] S. Amberkar, J. G. D'Ambrosio, B. T. Murray, J. Wysocki és B. J. Czerny, „A system-safety process for by-wire automotive systems," in *Safety-critical automotive systems*, Society of Automotive Engineers, Inc., 2006, pp. 13-18.

[8] A. Balogh Dr., „A rendszer-megbízhatóság műszaki tervezése," *Híradástechnika,* %1. kötetLIX, pp. 2-8, 2004.

[9] B. S. Dhillon, Reliability engineering in systems design and operation, Van Nostrand Reinhold Company Inc., 1983.

[10] D. D. Bell és S. J. Keene, „Software reliability: A continuing dilemma," in *Proc. of Annual Reliability and Maintainability Symposium*, Anaheim, 1998, pp. 215-230.

[11] M. Signor, „The failure-analysis matrix: A Kinder, gentler alternative to FMEA for information systems," in *Proc. of Annual Reliability and Maintainability Symposium*, Seattle, 2002, pp. 173-177.

[12] P. Goddard, „Validating the safety of embedded real-time control systems using FMEA," in *Proc. of Annual Reliability and Maintainability Symposium*, Atlanta, 1993, pp. 227-230.

[13] L. Travascio, M. Compare, G. Anna, G. Gigante és A. Vozella, „About the aerospace and aeronautics domains overlapping in safety issues," in *European safety and reliability conference; Risk, reliability and societal safety* , London, 2007.

[14] J. Rohács, Quick market analysis and foresight on aircraft brake system, 2005.