A rendszer-megbízhatóság műszaki tervezése

DR. BALOGH ALBERT

albert.balogh@axelero.hu

Egy rendszer megbízhatóságát számos egymással kölcsönhatásban lévő tényező határozza meg. Ezek közül a legfontosabbak a következők: alkotó elemek, alkatrészek, a rendszer szoftverje, az emberi hatások, az üzemeltetési profil, a rendszer üzemeltetésével kapcsolatos szolgáltatás minősége, a környezet. A Nemzetközi Elektrotechnikai Bizottság (IEC) 56. Műszaki Bizottsága (TC 56) javaslattervezetet dolgozott ki a rendszer megbízhatóságának műszaki tervezése során alkalmazandó irányelvekre. A jelen közlemény ezen útmutató [1] alapján foglalja össze a rendszer-megbízhatóságra ható tényezőket és azokat a módszereket, amelyekkel a kitűzött megbízhatósági célok elérhetők.

1. Bevezetés

Az irányelvek széleskörűen alkalmazhatók különböző rendszerekre, így például távközlési-, szállítási-, termelési rendszerekre. Az ismertetés kitér a szervezési és műszaki kérdésekre is, valamint arra is, hogy ezek hogyan kapcsolódnak a megbízhatósági célok elérésére alkalmazott módszerekhez és eszközökhöz. Különbséget kell tenni a szervezési és irányítási (menedzselési) tevékenységek között attól függően, hogy milyen hatást gyakorolnak a rendszer megbízhatóságára.

A rendszert az ISO 9000:2000 szabvány [2] a következőképpen határozza meg: „Egymással kapcsolatban vagy kölcsönhatásban lévő elemek összessége adott cél elérésére."

A rendszert hierarchikus felépítésűnek tekintik, így egy termék lehet rendszer vagy részrendszer (alkatrész, elem) attól függően, hogy milyen szinten vizsgáljuk a rendszer leírását, azaz a terméket részeire bontjuk (rendszer) vagy sem (elem). A rendszer tervező első lépése az, hogy meghatározza rendszer feladatait és azokat lebontsa részrendszerekre.

2. A rendszer-megbízhatóság műszaki tervezésével kapcsolatos fogalmak

2.1. Általános alapelvek

A tervezése arra irányul, hogy egy vagy több adott célt és rendeltetés szerinti feladatot teljesítsen a rendszer. A rendszer-megbízhatóság ugyan a rendszer belső eredetű jellemzője, mégis csak akkor értelmezhető, ha adott cél elérésére vonatkoztatjuk. A rendszer megbízhatósági elemzését azzal célszerű kezdeni, hogy egyértelműen meghatározzuk a különböző rendeltetés szerinti feladatokat és azok teljesítésének feltételeit.

Ezeket a feladatokat rendszerint a követelmények szabványában adják meg. Ezen túlmenően vannak magától értendő teljesítendő tulajdonságok is. A rendszer állapota akkor hibás, ha megkövetelt funkcióinak legalább egyikét nem tudja ellátni. A rendszer fejlesztési projekt egyik legfontosabb célja olyan rendszer kidolgozása, amelynek minősége és megbízhatósága megfelel a követelményeknek.

2.2. Az alkotó elemek közötti kölcsönhatások

A rendszer megbízhatósága nemcsak alkotó elemeinek megbízhatóságától függ, hanem az azok között fellépő kölcsönhatásoktól is. Például a tartalékolás megbízhatóságot növelő pozitív hatás, ugyanakkor több alkatész együttes, egymástól függő meghibásodása csökkenti a rendszer megbízhatóságát. Ha egy bonyolult rendszert vizsgálunk, akkor nem elegendő figyelembe venni az egyes alkatrészek megbízhatóságát, hanem azt is számításba kell venni, hogy azok kölcsönhatása hogyan befolyásolja a rendszer-működését. Például az emberi beavatkozás miatt kialakult tervezési hibák üzemeltetési hibához vezethetnek.

Annak elérésére, hogy megbízható rendszert fejlesszünk ki és értékelni tudjuk, hogy az megfelelő-e vagy sem, mennyiségi megbízhatósági célokat kell kitűznünk. Ezen célok teljesítését ellenőriznünk kell a megcélzott alkalmazási körülmények között. A megbízhatóság gyűjtőfogalom, amely több tulajdonságra vonatkozik, ezért önmagában nem számszerűsíthető. A mérőszámok azonban az egyes tulajdonságokra meghatározhatók, melyeknek szintje függ attól, hogy milyen követelményt támasztanak azokkal szemben. Például a veszélyes folyamatok ellenőrző rendszerének az átlagosnál nagyobb használhatósággal és hibamentességgel kell rendelkeznie.

A részrendszerek között úgy kell felosztani a megbízhatósági követelményeket, hogy azok megfeleljenek az egész rendszerre előírt megbízhatósági követelménynek, de legolcsóbban legyen realizálható. Fontos figyelembe venni, hogy a rendszer megbízhatósága változik az üzemeltetési környezettől függően. Ez hat azokra az igénybevételi feltételekre, amelyek között a rendszer és részegységei, alkatrészei működnek. Ebből adódik, hogy a környezet befolyásolja a különböző meghibásodások előfordulási valószínűségét is.

2.3. A szoftver fontossága

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

Az IP alapú hálózatok működését meghatározó routerek, bridgek, switchek és szerverek szoftverjeinek megbízható működésére kiemelt figyelmet kell fordítani. Itt a hibák felderítése hosszadalmas, sok futtatást igénylő feladat. Ezek vizsgálata tudományos körültekintést igényel [5,6,7,8].

2.4. Emberi hatások

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:

a) Beavatkozás a rendszer ember-gép kapcsolat során.
b) Beavatkozás a hálózaton keresztül (például egy másik rendszer ember-gép kapcsolatából kezdeményezték vagy a távközlési hálózat különböző pontjain végzett munkák hatása).
c) Beavatkozás, amely fizikailag a környezetből történik, eltérően az ember-gép kapcsolatból származó beavatkozásoktól.

Az ember-gép kapcsolatra a következő megbízhatósági követelmények vannak:

- Legyen védelem a rendszer illegális elérése és az illegális belépés ellen.
- Legyenek világosan érthető felhasználási utasítások.
- Legyen 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 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.

2.5. Üzemeltetési profil

Az üzemeltetési profilt a konfigurációk (kiépített kapcsolatok a rendszerben), a működési állapotok és a környezeti feltételek összessége határozza meg. Ezek a tényezők szükségesek a rendszer funkciónak ellátásához. A rendszer üzemeltetési profiljának elemzése a rendszerkövetelményekre és a kereskedelmi vonatkozásokra is kiterjed.

2.6. A szolgáltatás-minőség (QoS) és a rendszer-megbízhatóság kapcsolata

A szolgáltatás-minőség (Quality of Service, QoS) a rendszer általános teljesítmény mutatója. A QoS és a rendszer-megbízhatóság egymást átfedő fogalmak. Kapcsolatukat ismerni kell és ez alapvetően fontos a rendszer-megbízhatóság műszaki tervezése során. Az ITU-T Recommendation E. 800 [3] határozza meg ezt a kapcsolatot.

Ez látható a 6. pont *3. ábráján,* amely megadja a megbízhatósági és szolgáltatás-minőségi jellemzők négyszintű integrált tartományát, ahol a 3. szint jeleníti meg az átfedés területét.

2.7. A környezet hatása

A rendszer-megbízhatóságot mindig jelentősen befolyásolja a környezet. Ezért a rendszer műszaki előírásaiban meg kell határozni az üzemeltetés környezeti feltételeit, melyeket a kockázat és a megbízhatóság elemzése során figyelembe kell venni. A környezeti megfontolásokat érvényre kell juttatni az elavulás és a termék selejtezése szakaszában is.

Az elemzési módszerek összehangolása során a különböző elemzési módszereket, mint például a hibafa-elemzés (FTA), a meghibásodási mód, -hatás és -kritikusság elemzése (FMEA), a veszélyhelyzeteket és üzemeltethetőség vizsgálatokat (HAZOP) és a megbízhatóság előrejelzését, együtt kell áttekinteni.

Konfiguráció-menedzsment (rendszerek közötti kapcsolat kiépítésének irányítása) és menedzselése a megbízhatóság egyik legfontosabb kérdése. Példa erre a karbantartást ellátó szervezet létrehozása és rendszerhez való kapcsolása. Ezek a különböző konfigurációk által előállított kapcsolatok nagyon változatosak. Közvetlen kereskedelmi hatása van például annak, hogy az alkatrészek felcserélhetőségére és a rendszerek együttes működtetésére vonatkozóan egyre szigorúbb követelmények vannak. Ez különösen igaz hosszú élettartamú (például távközlési) rendszerekre, amelyeknek gyorsan avuló alkatrészei vannak, vagy amelyeknél technológiai változtatásokat végeznek. Ugyanakkor a hálózat különböző részeiért más üzemeltetők felelősek.

Teljesítőképesség (műszaki kapacitás) azt jelenti, hogy megfelelően méretezett erőforrások állnak rendelkezésre a rendszer által megkövetelt bármely szolgáltatási igény teljesítésére (például a karbantartó szervezet munkaerő és kapacitása). Ezek befolyásolják a szolgáltatás elérhetőségét és folyamatosságát. Ajánlatos a hibák súlyozása az általuk okozott rendszer-teljesítőképesség csökkenésének mértéke szerint.

A teljesítőképesség csökkenését az egész teljesítőképesség százalékában kell megadni. Itt kell figyelembe venni a forgalmi méretezést [9,10].

3. A megbízhatósági képességek (tulajdonságok) és azok mennyiségi jellemzői

A megbízhatósági fogalmakat az MSZ IEC 50(191) szabvány [4] határozza meg. A megbízhatósági képességekhez mérőszámokat rendelnek hozzá. A *megbízhatóságot meghatározó képességek* (használhatóság, hibamentesség, karbantarthatóság, karbantartás-ellátás, valamint a [4]-ben nem szereplő alkalmazhatóság, biztonság, adatbiztonság, hatékonyság) a felhasználónak azt az elvárását tükrözik, hogy káros események (meghibásodások, incidensek) milyen valószínűséggel fordulnak majd elő az üzemeltetés során.

A következőkben tárgyalandó fogalmak esetében az esemény lényeges voltát annak okai, módja, hatása és következménye szigorúsági fokozata határozza meg. Csoportosításuk a következő:

- Ha a meghibásodást nem tervezett (szándékos) hiba idézi elő és nem jelent veszélyt emberéletre és vagyonbiztonságra, valamint a környezetre, akkor „közönséges" meghibásodást jelent és a *hibamentesség* szempontjából lényeges.
- Ha a hiba a felhasználónál jelentkezik, amikor az igénybe akarja venni a szolgáltatást és ennek következtében a felhasználó képtelen a feladatok végrehajtására, akkor a meghibásodás az *alkalmazhatóság* szempontjából lényeges.
- Ha a hiba az élet- és vagyonbiztonságot veszélyeztető kritikus meghibásodást eredményez, akkor a *biztonság* szempontjából lényeges.
- Ha a hiba szándékos rendszer elleni támadást jelent és veszélyezteti az információbiztonságot, akkor a meghibásodás az *adatbiztonság* szempontjából lényeges.

A következőkben ismertetjük ezen meggondolások alapján a megbízhatósággal kapcsolatos fogalmakat a [4] szabvány alapján.

3.1. Megbízhatóság (Dependability)

Gyűjtőfogalom, amelyet a használhatóság (üzemkészség, rendelkezésre állás) és az azt befolyásoló tényezők, azaz a hibamentesség, a karbantarthatóság és a karbantartás-ellátás leírására használnak.

Ez a fogalom a termék időtől függő képességeit öleli fel, mennyiségi leírásra nem használható.

3.2. Hibamentesség (Reliability)

A terméknek az a képessége, hogy előírt funkcióit adott feltételek között, adott időszakaszban ellátja.

Mennyiségi jellemzői: *az R(t) hibamentes működési valószínűség (túlélési valószínűség), amely megadja annak valószínűségét, hogy a termék a t időpontot túléli, meghibásodási valószínűség, a $\lambda(t)$ meghibásodási ráta, meghibásodások közötti átlagos működési idő.*

A működési idő nem azonos általában a naptári idővel. A működési időt különböző mértékegységekben mérhetik (gépkocsi esetében a megtett km-ek számával, repülőgépek esetében a repülési órák számával, a távközlésben a sikeres kapcsolás felépítések számával. Szoftverek esetén a végrehajtási idővel, a programok előhívási számával, a végrehajtott utasítási ciklusszámmal lehet mérni a működés tartamát).

Az átlagos működési időt az első meghibásodásig (Mean Time To First Failure, MTTFF) főként nem javítható termékek esetében használják a meghibásodások közötti átlagos működési időt (Mean Time Between Failures, MTBF) javítható termékek esetében alkalmazzák. A működési idő exponenciális valószínűségi eloszlása esetén az MTBF (MTTFF) értéke a λ meghibásodási ráta reciprokával egyenlő, exponenciális eloszlás esetében λ állandó.

3.3. Karbantarthatóság (Maintainability)

A karbantarthatóságot a karbantartás adott (t) idő alatti elvégzésének M(t) valószínűségével és a javítási rátával jellemzik. A valószínűségi eloszlásból származtatják a többi jellemzőt a következők szerint:

Mennyiségi jellemzői: *átlagos javítási idő (Mean Repair Time, MRT), átlagos helyreállítási idő (Mean Time To Restoration, MTTR).*

A javítási idő vonatkozhat a javító karbantartás idejére, de szorítkozhat csak a javítás elvégzésének idejére. A javító karbantartási idő a felkészülési késedelem, a műszaki késedelem és a javítás tényleges elvégzése idejének összegével egyenlő.

A karbantartás fajtái a következők: megelőző-, javító-, alkalmazkodó- (új környezetben is tudja szolgáltatásait teljesíteni a rendszer), fejlesztő- (a rendszer változtatása, hogy növelje a rendszer szolgáltatás-minőségének megkövetelt szintjét) karbantartás. Szoftver esetében csak javító karbantartást végeznek.

A hardver karbantartása a személyzet és a karbantartáshoz szükséges anyagok mozgatását követeli meg. A szoftver karbantartása az információk mozgatását (továbbítását) igényli. A szoftver javított változatait a felhasználó otthonában (a helyszínen) le tudja tölteni.

3.4. Karbantartás-ellátás (Maintenance support)

A karbantartó szervezetnek az a képessége, hogy adott feltételek között – igény esetén – rendelkezésre bocsátja azokat az erőforrásokat és eszközöket, amelyek a termék karbantartásához szükségesek.

Mennyiségi jellemzői: *átlagos karbantartási munkaidő-ráfordítás, átlagos késedelmi idő (várakozás a javítás, karbantartás megkezdéséig).*

A karbantartást ellátó szervezetnek hardver esetében a következő feladatai vannak: tartalék-alkatrészek beszerzése, helyszínre szállítása és a karbantartó személyzet kiszállása (felkészülési késedelem), a rendszer javításra való felkészítése (műszaki késedelem), javítás elvégzése, helyreállítási vizsgálat (ellenőrzés). Szoftver esetében a feladatok a következők: a hiba bejelentés fogadása és a javító szakember kijelölése felkészülési késedelem), a vizsgálati hely kijelölése a diagnosztikai program lefuttatására (műszaki késedelem), a javított szoftver elkészítése, helyreállítási vizsgálat és a javított szoftver próbafuttatása, átvitele és ellenőrzése.

3.5. Használhatóság, rendelkezésre állás (Availability)

A terméknek az a képessége, hogy adott időpontban vagy időszakaszban, adott feltételek között ellátja funkcióit. Ez azt jelenti, hogy a terméket adott időpontban használatba tudjuk venni és ezt követően folyamatosan használni tudjuk. Ennek mennyiségi jellemzője a használhatóság valószínűsége, amelyet az A(t) használhatósági függvény ír le. Az A(t) függvény értékének 1-hez közelinek kell lennie. Ehhez egyrészt hosszú idejű hibamentes működés, másrészt rövid idejű karbantartás (megelőző vagy javító karbantartás) szükséges.

Ezért a használhatóság mennyiségi jellemzője közelítéssel az állandó stacionárius vagy aszimptotikus *használhatósági tényező,* amely azt fejezi ki, hogy a terméket az esetek hányad részében tudja a felhasználó működőképesen használni, ez képletben a következő:

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

További megbízhatósággal kapcsolatos időfogalmak: *élettartam, illetve üzemidő (Life Time),* amely a működési idők összege a termék használatba vételétől a határállapotig. Határállapot az az állapot, amelyben a termék működését be kell szüntetni, mert vagy veszélyben van az élet- és vagyonbiztonság, vagy elavult a termék, gazdaságtalan a működtetés, teljes tönkremenés (totálkáros gépkocsi). A köznapi nyelvben, de a gyakorlatban is használják a *naptári idő* fogalmát, ekkor a termék használatba vételétől a határállapotig eltelt naptári időt veszik figyelembe, például a jótállási időt. Egy távközlési rendszer élettartamát is a naptári idő függvényében célszerű vizsgálni, ezért ezt a naptári időt szokták élettartamnak is nevezni.

3.6. A használhatóságot és az eszköz megítélését befolyásoló jellemzők

A következő további képességeket is figyelembe kell venni a rendszer-megbízhatóság műszaki tervezése során:

Alkalmazhatóság, más szóval kezelhetőség, használhatóság (Usability) – nem tévesztendő össze az üzemkészséggel. Az alkalmazhatóság az a képesség, hogy a felhasználó a szolgáltatást igénybe tudja venni.

Mennyiségi jellemzője: annak valószínűsége, hogy a felhasználó a megkövetelt funkciót sikeresen elő tudja hívni adott időszakaszon belül. Egy másik mérőszám az alkalmazhatóságra a következő: a feladat végrehajtásához szükséges idő. *Ezt lehet megtanulhatóságnak is nevezni (Learnability).*

Helyreállíthatóság (Recoverability, Restorability): a rendszernek az a képessége, hogy a meghibásodást követően helyreáll működőképessége és újra ellátja szolgáltatásait, függetlenül attól, hogy javító karbantartást végeztek-e vagy sem. Ezt feléleszthetőségnek is nevezik.

Mennyiségi meghatározása: annak valószínűsége, hogy a termék a meghibásodást követően ismételten ellátja megkövetelt szolgáltatásait adott feltételek között, adott időszakaszon belül, függetlenül attól, hogy javító karbantartást végeztek-e vagy sem. A helyreállíthatóság és az ezzel kapcsolatos javító karbantartás a hardver meghibásodásra, feléleszthetőség pedig a szoftver helyreállíthatóságára vonatkozhat.

Biztonság (Safety): a termék képessége az élet- és vagyonbiztonságot eredményező kritikus meghibásodások elhárítására. Mennyiségileg ezt nem jellemzik, mivel ennek nagy valószínűséggel kell teljesülnie.

Hatékonyság (Efficiency): annak mértéke, hogy a termék egy adott feladatot milyen hosszú idő alatt végez el.

Adatbiztonság (Security): az illegális behatolások elhárításának képessége.

Mennyiségi jellemzője: annak valószínűsége, hogy adott behatolást (támadást) sikeresen elhárítanak adott feltételek között, adott időn belül. Az [1] hivatkozás a behatolás sikerességének valószínűségét, azaz az adatbiztonság megsértésének a valószínűségét méri.

4. Hibaállapot, hiba és meghibásodás

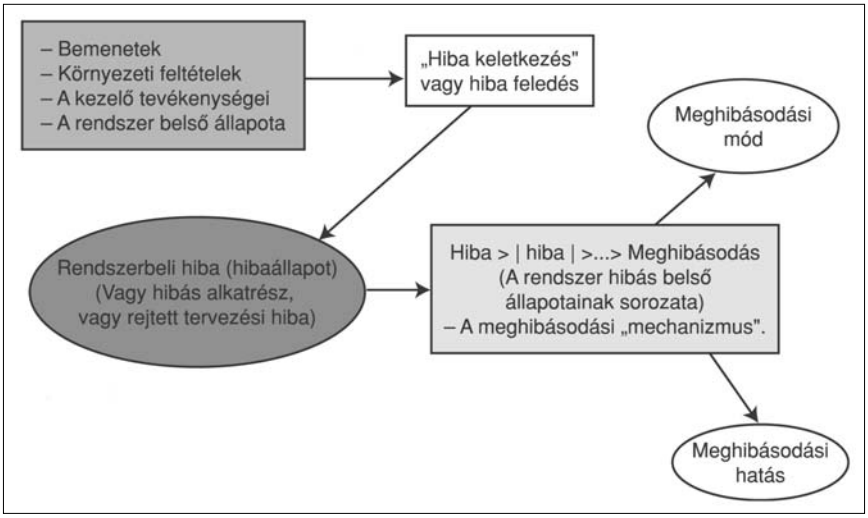
A következő oldalon, az *1. ábrán* látható az a kapcsolat, amely a hibaállapot, röviden: hiba (fault), a meghibásodási mechanizmus (failure mechanism) hatásaként keletkező meghibásodás (failure), annak módja (mode) és hatása (effect) között jön létre.

A rendszert meghibásodottnak tekintik, ha időlegesen vagy véglegesen nem látja el előírt funkcióit. A meghibásodás eseménye az okok sorozati láncának végpontján van.

Ez a folyamat a rejtett tervezési hiba feléledésével kezdődik (hiba-keletkezésnek nevezik), ezt követi a hibás belső állapot vagy azok sorozatának (ezt is hibának nevezzük, angol megfelelője: error) elterjedése a rendszerben. Ha hibás belső állapotot nem fedezik fel és nem javítják ki a rendszer tervezése során beépített *hibatűrő* tulajdonságok felhasználásával, akkor a hiba addig terjed, ameddig az rendszer-meghibásodást nem okoz.

A *tervezési hibák beépítésének hat szintje* van:

1. szint: a leírt követelmény nem felel meg a felhasználó „valós” követelményének (jelentős hibákat vihet be a rendszerbe).
2. szint: a rendszer általános tervezése nem megfelelő (hiányzik a hibatűrés). A rendszert lehet, hogy ellenőrizték és igazolták („ Jól építettük fel a rendszert?”), de lehet, hogy nem alkalmas módon hagyták jóvá („A megfelelő rendszert építettük fel?”).
3. szint: a tervezés nem felel meg a leírt követelményeknek.
4. szint: a felépített rendszer nem felel meg a részletes tervezésnek.
5. szint: kódolási hibák vannak a tervezésben.
6. szint: a nem gondos karbantartás új hibákat vezethet be.



1. ábra
A meghibásodási típusok elvi modellje

A *tervezési meghibásodások jellege* általában az alábbiak egyike:

a) Ember által előidézett meghibásodás:
kódolási hiba vagy karbantartási hiba.
b) Átmeneti (időleges) meghibásodás:
megszűnik, ha a keletkezés okát megszüntetik.
c) Rendszeres meghibásodás:
újra jelentkezik, ha az oka ismét előfordul.
d) Véletlen meghibásodás:
a keletkezés feltételei véletlenül fordulnak elő.
e) Rejtett hibaállapotok miatt fellépő meghibásodás:
a hiba feléledése miatt lép fel.
f) Ritka meghibásodás:
a keletkezés feltételei nem gyakran fordulnak elő.
g) Előre nem jelezhető meghibásodások:
ezek elhárítására nehéz védelmi eszközöket a rendszerbe tervezni és beépíteni.

A koncepcióbeli meghibásodásokhoz (a tervezési hiba miatti meghibásodásokhoz) vezető folyamatok és azok kapcsolatai a hiba-fogalmakkal a *2. ábrán* láthatók.

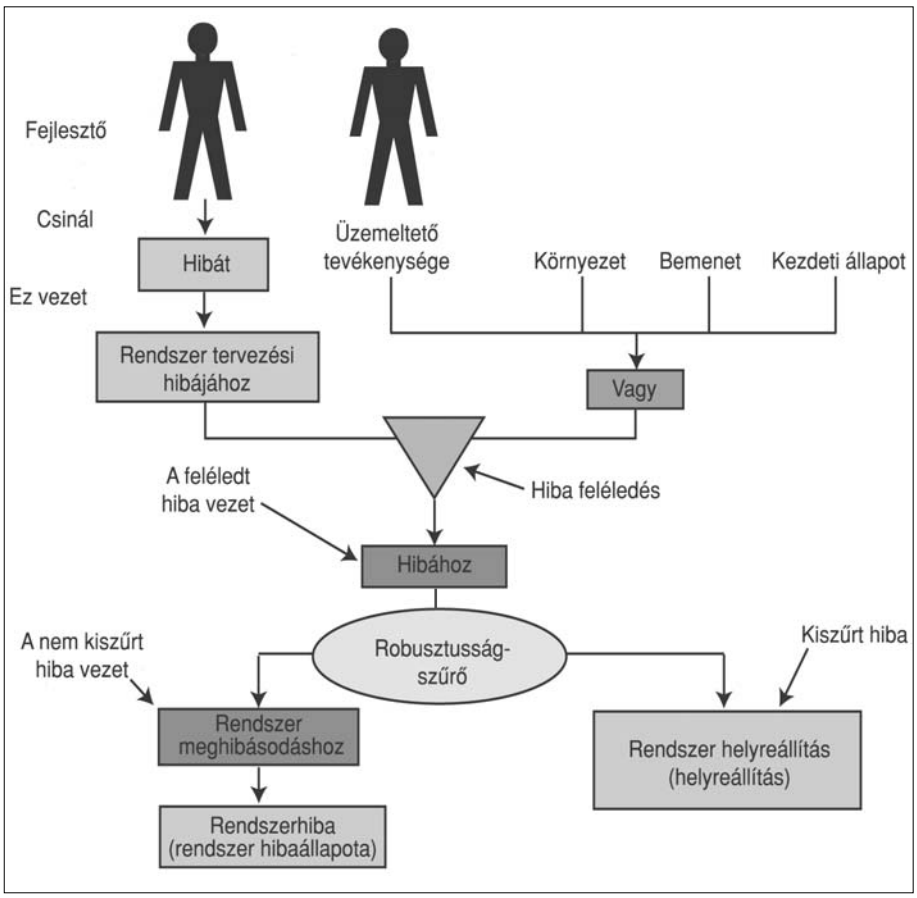
5. A megbízhatóság és a rendszer életciklus-szakaszai közötti kapcsolat

5.1. Általános áttekintés

A megbízhatóság-menedzsment (megbízhatóságirányítás) elősegíti kölcsönös kapcsolat létrehozását 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 rendszer megbízhatóságát a [4] szabványban megadott mennyiségi jellemzők alapján kell értékelni az előírt érték és az elért eredmény összehasonlításával.*

5.2. A megbízhatóság biztosítása

A bonyolult rendszerek meghibásodását vagy valamely alkotó részhibája, vagy rejtett tervezési hiba idézheti elő.



2. ábra
A koncepcióbeli (vagy a tervezési) meghibásodásokra vonatkozó „hiba (tévedés)", „hiba (hibaállapot)", „hiba" és „meghibásodás" fogalmak közötti kapcsolat

Ezért a rejtett tervezési hibák bekövetkezésének valószínűségét és feléledésüknek káros hatását a lehető legkisebbre kell csökkenteni. Ennek teljesüléséről biztosítékot kell nyújtani a leendő vevő számára, ezt a bizalomkeltési tevékenységet nevezik megbízhatóságbiztosításnak.

Három módszer van a rejtett tervezési hibák csökkentésére: a hiba elkerülése, a hiba eltávolítása és a hibatűrés (hibatűrő-képesség).

A tervezési hibákat elsődlegesen „jó tervezési gyakorlat"-ot követve hárítják el. Lényeges, hogy a vevő „tényleges" követelményeit a rendszer prototípusának alkalmazása és értékelése során érvényesítsék. A legsúlyosabb üzemeltetési meghibásodások a követelmények meghatározásában talált hiányosságoknak tulajdoníthatók. A jó tervezési gyakorlatot követve az egyes részegységek összehangolását az általános tervezési szinten kell elvégezni és a részletes tervezésben el kell kerülni az egymással kapcsolatban lévő részegységek felesleges kettőzését. Külön gondot kell fordítani a felhasználó-barát interfészek tervezésére. A szoftver változtatása után helyreállítási tesztet kell futtatni, hogy elkerüljük az új hibák beépítését, amikor megkíséreltük előzőleg a régi hibákat eltávolítani. A legjobb tervezési gyakorlat sem szavatolhatja a kiküszöbölését. A hibákat ezért már a fejlesztés során automatizált elemzési módszerekkel és a fejlesztés mindegyik szakaszában végzett ellenőrzésekkel el kell távolítani. Ezzel elkerülhető a hibák átvitele egyik szakaszból a következő szakaszba.

Az alapos ellenőrzést a felhasználói feltételeket jól közelítő (szimuláló) kísérleti üzemeltetés követi. A vizsgálatot részegységenként (modulonként), a nagyobb részrendszerek integrálása után kell elvégezni, végül pedig a teljes rendszert kell jóváhagyni a felhasználó követelményei szerint, még a szolgáltatás megkezdése előtt.

A rendszer üzemeltetésére olyan eljárásokat kell kidolgozni, amelyek lehetővé teszik a felhasználók számára a meghibásodás bejelentését úgy, hogy a szervizelő szervezet személyzete megállapíthassa a hiba okát és ennek alapján módosításokat végezzen a rendszerben azok eltávolítására.

A rendszer bemeneteinek és belső állapotainak száma igen nagy, ezért a hibák eltávolítása sem adhat tökéletes eredményt. Ezért hibatűrő rendszert kell tervezni, amelynél a rendszer egyik alkotó elemének hibája a többi alkotóelemet ne befolyásolja. A hiba így megszüntethető mielőtt a rendszerben elterjedne és a rendszer meghibásodna. Ez védelmi tervezést és programozást jelent, valamint tartalékegységek (modulok) beépítését teszi szükségessé azért, hogy a többi egység állapota ellenőrizhető legyen. *A hibatűrés beépítése biztosítja a rendszer hibahatás elleni védettségét és hibahatástól mentes működését.*

5.3. A rendszer-megbízhatóság vizsgálata az egyes életciklus-szakaszokban

A rendszer valamennyi életciklus-szakaszában meg kell vizsgálni a megbízhatóság, biztonság és adatbiztonság követelményeinek teljesülését.

A *rendszer tervezése és fejlesztése* során a részrendszerek megbízhatóságával érhető el, azok integrálása során, a megkövetelt rendszer-megbízhatóság. A biztonság kérdéseivel a közlemény alapjául szolgáló [1] dokumentum nem foglalkozik, az adatbiztonság kérdéseit csak érinti. A rendszer fejlesztését a megbízhatóság-növelési programmal összehangolva kell elvégezni. A tervezéskor gondot kell fordítani arra, hogy az alvállalkozói szerződések megbízhatósági követelményeket is tartalmazzanak.

A *rendszer gyártása* során figyelembe kell venni a jó vevő-szállító kapcsolat kialakítását, az üzemeltető és karbantartó személyzet képzését.

A *rendszer üzemeltetése és karbantartása* során a rendszer-megbízhatóságot befolyásoló tényezők a következők lehetnek: a rendszer üzemmódja, a rendszer együttes működtetése más rendszerekkel, karbantartás és karbantartás-ellátás, emberi hatások.

A *rendszer selejtezése* során a megbízhatóságra vonatkozó információkat gondosan meg kell őrizni, a selejtezést a környezet károsítása nélkül kell elvégezni.

6. Összefüggés a szolgáltatás minősége (QoS) és a rendszer megbízhatósága között

6.1. Általános fogalmi megfontolások

A rendszer üzemeltetésének célja az, hogy szolgáltatást nyújtson a felhasználó részére. A felhasználók akkor veszik igénybe a szolgáltatást, ha annak jellemzői (minősége) megfelelnek elvárásaiknak. A szolgáltatás-minőséget fontos tényezőnek kell tekinteni a tervezés során.

A rendszer megbízhatóságának és a szolgáltatás minőségének kapcsolatát [3] és [4] szabványok határozzák meg. A 2. pontban részletesen foglalkoztunk a hibamentesség, a karbantarthatóság és a karbantartás-ellátás fogalmainak, valamint azok együttes hatását leíró használhatóságnak meghatározásával. Az első három összetevő jelenti a QoS és a megbízhatósági jellemzők legalsó hierarchia-szintjét a *3. ábrán*. A használhatóságot az ábrán a 2. hierarchia- szint jeleníti meg. Ez pedig azt eredményezi, hogy a rendszernek késznek kell lennie a szolgáltatás teljesítésére. Ha nem üzemeltethető a rendszer, akkor nem tud szolgáltatást nyújtani. A rendszer szolgáltatás-minőségét a 3. szinten kell vizsgálni. Ez a rendszer használhatóságának szintje felett van. Minden szolgáltatás minőségét több fogalom együttesen írja le. Ezek közül két fontos QoS fogalmat kell kiemelni:

Szolgáltatás elérhetősége (Service accessibility)

A szolgáltatásnak az a képessége, hogy – adott tűréseken belül és adott feltételek között – megkapható, ha a felhasználó igényli.

Szolgáltatás folyamatossága (Service retainability)

Az egyszer már megkapott szolgáltatásnak az a képessége, hogy adott feltételek között, kívánt időtartamig folytatódik.

Ez a két fogalom a szolgáltatás használhatósági jellemzőjeként is értelmezhető, ha a szolgáltatást teljesítő rendszerek rendelkezésre állnak. Ezért ez a két jellemző nemcsak QoS fogalom, hanem használhatósági fogalom is a 3. szinten.

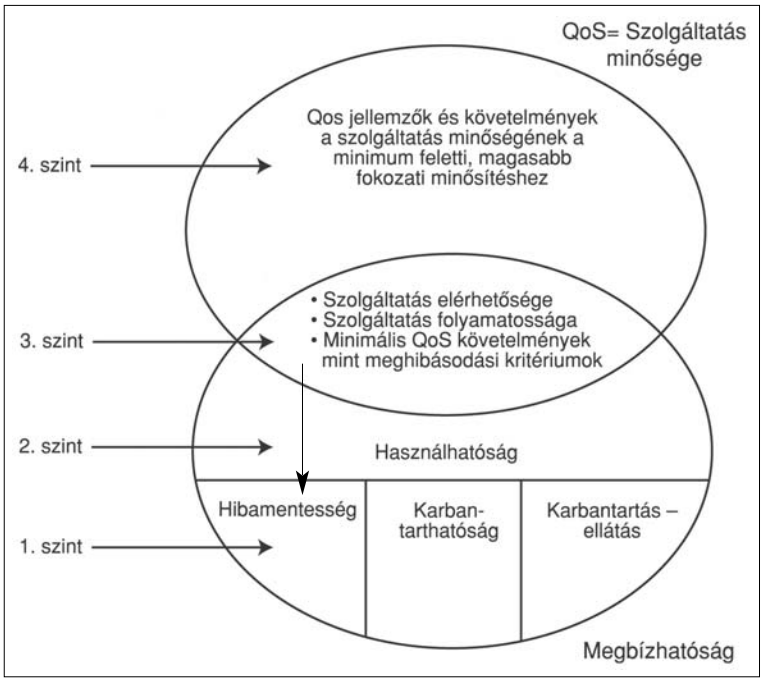
A QoS és a rendszer-megbízhatóság tervezésének további közös területei is vannak. A minimális QoS követelmények nem teljesítése meghibásodásnak tekintendő, ezért a műszaki tervezés során ezt meghibásodási kritériumként kell figyelembe venni. A QoS azonban többet jelent a megbízhatóságnál, mert tovább osztályozza az egyes rendszer-szolgáltatásukat minőségük szerint a minimális minőség-szint felett. Ennek azonban előfeltétele, hogy a QoS-hez mérhető, objektív minőségi paramétereket rendeljünk. Ezeket a *3. ábra* 3. és 4. szintjén szereplő jellemzőkre osszuk fel és az összegezési szabályokat előre rögzítsük. Ezáltal további különbséget tehetünk a másképpen azonosan „megbízható" rendszerek között. A megbízhatósági és QoS jellemzők egyesített modellje a *3.ábrán* látható.

6.2. A megbízhatóság műszaki tervezésének fontossága

A rendszer-megbízhatóság műszaki tervezése a minimális QoS szint figyelembe vételével kezdődik. A rendszer egyes előírt funkcióira megbízhatósági jellemzőket kell megállapítani.

Ezek lehetnek a következők: használhatóság, állási idő, MTTR. Ezt követően osztályozni kell a különböző hibatípusokat jelentős és jelentéktelen, teljes és részleges hibák. Ezt követően az általános követelményeket fel kell osztani minősítéses és mennyiségi követelményekre. A megbízhatósági vizsgálatoknak is arra kell irányulniuk, hogy igazolják a szolgáltatás használhatóságára vonatkozó követelmények teljesülését.

3. ábra A megbízhatóság és a szolgáltatás-minőség jellemzőinek négy szintű integrált tartománya



7. A rendszer életciklusának folyamatai

A megbízhatóság-irányítás a rendszer életciklus folyamatait használja fel a megfelelő megbízhatósági folyamatok irányítására. A folyamatok négy csoportra oszthatók fel:

1. Vállalati folyamatok, amelyek kiterjednek a vállalat-, a befektetés- és az életciklus-irányítási, valamint az erőforrás-gazdálkodási folyamatokra.
2. Szerződéses folyamatok, amelyek tartalmazzák a beszerzési- és a szállítási folyamatokat is.
3. A projekt irányításának folyamatai felölelik a tervezési-, értékelési-, szabályozási-, döntéshozási-, kockázatkezelési-, konfiguráció-kiépítési- és minőségirányítási folyamatokat.
4. A technikai folyamatok a következők: az érdekelt felek igényeinek meghatározását, a követelmények elemzését, a tervezést, integrálást, igazolást, telepítést, jóváhagyást, és selejtezést egyaránt tartalmazzák.

Irodalom

[1] IEC TC 56 (2004):
Guidance to Engineering of System Dependability

[2] ISO 9000:2000: Quality Management Systems:
Fundamentals and Vocabulary (2000)

[3] MSZ ISO 50(191):
Megbízhatóság és szolgáltatásminőség fogalmai (1993)

[4] ITU-T Recommedation E 800

[5] Methods for Testing and Specification (MTS);
Testing and Test Control Notation; Part 1:
TTCN-3 Core Language, ETSI ES 201 873-1.

[6] Gecse R.–Szabó J.–Csöndes T.:
Időzített véges automata alapú vizsgálati módszer.
Híradástechnika 2002/3., pp.19–24.

[7] Andriska Z.–Bátori G.–
Wu-Hen-Chang A.–Csopaki Gy.:
Automatikus tesztkiválasztás
formális specifikáció alapján

[8] Lócz B.–Zömbik L.:
Hálózati protokollok biztonsági tesztelése.
Híradástechnika 2004/3., pp.2–9.

[9] Konkoly Lászlóné–Fekete I.:
Nyereség optimalizálás
az üzleti kockázatelemzés és játékelmélet
együttes alkalmazásával.
Híradástechnika 2003/9., pp.4–11.

[10] Molnár S.–Szabó Z.–Kenesi Zs.:
Aktív tároló kezelő mechanizmusok
hatása a TCP adaptivitásra.
Híradástechnika 2003/4., pp.15–24.

[11] Ornicsay D.–Józsa B.:
Távközlési hálózatok
költséghatékony tervezése.
Híradástechnika 2003/4., pp.25–29.

[12] Kanász-Nagy L.:
Biztonság a távközlésben.
PKI Közl., 48. szám, 2004., pp.141–154.