REPÜLÉSTUDOMÁNYI KÖZLEMÉNYEK
35. évfolyam (2024) 2. szám 19–46. • DOI: 10.32560/rk.2024.2.2

Beller Balázs

A repülésbiztonsági kockázatelemzési eljárások evolúciója II.

Mint sok veszélyes üzem, a légi közlekedés is csak elfogadott és elfogadhatatlan, azaz kezelendő kockázatok mentén valósítható meg. A cikk megírásának célja, hogy folytassa az 1960-as évektől megjelenő kockázatelemzési eljárások bemutatását, esetleges egymásra épülését, használhatóságát. Ismertetni kívánja azon kockázatelemzési és szemléltetési eljárásokat, amelyek a lineáris kockázatelemzési eljárásokon túl a komplex, többszörösen összetett rendszerek elemzésére is alkalmazhatók. A 2000-es évek után megjelenő modellek megértése, alkalmazása ugyanakkor legalább annyira nehéz, összetett feladat, mint azon rendszerek megértése, amelyek elemzésére ezen modellek készültek. A cikk többek között ezen komplex látásmód megértésében is próbál segítséget nyújtani. A választott kutatási módszer alapvetően a külföldi szakirodalom feldolgozásán alapult.

Kulcsszavak: *kockázatelemzés, kockázatok kezelése, lineáris eseménymodell, komplex nemlineáris eseménymodell, FRAM, STAMP, STPA*

1. Bevezetés

A cikk első részében áttekintettem a lineáris, ok-okozati kockázatelemzési eljárásokat, amelyek az 1960-as évektől kezdődően fejlődtek, és alkalmazásuk a 1970-es évektől válhatott általánossá. Ezen kockázatelemzési eljárásokat jelenleg is használják a légi közlekedés területén, annak ellenére, hogy azok gyökerét adott esetben más iparágak, veszélyes üzemek és folyamatok tervezése, végrehajtása során dolgozták ki. A tapasztalatok alapján ugyanakkor igény van a kockázatelemzési eljárások fejlesztésére is, kiváltképpen akkor, ha a vizsgált rendszerek, folyamatok komplexitása, integráltsági foka egyre magasabb szinteket ér el.

Egy bizonyos összetettségi szint felett problémát jelentenek a lineáris modellek korlátai, amelyekkel az erősen szoftverközpontú rendszerek elemzése csak egyszerűsítve dolgozható fel, és szükség volt és van ezen rendszerek elemzését is lehetővé tevő technikák kialakítására.

2. Baleseti modellek

A kockázatelemzési eljárások jelentős részben már egy korábban meglévő eseményelemzési – balesetek ok-okozati összefüggésének megállapítására szolgáló – modellre épülnek.

A kockázatelemzési eljárásokhoz használt modellek jelentős részét megtaláljuk a balesetek ok-okozati összefüggéseinek leírására használt modellek között. A balesetelemzési modellek fejlődése pedig alapvetően nyomon követhető a kockázatelemzési eljárások fejlődésén keresztül is, hiszen az események vizsgálatához hasonló elemzési eljárásra van szükség ahhoz, hogy a bekövetkezni vélt események kockázatait fel lehessen tárni. Természetesen nem minden eseménymodell alkalmazható teljes mértékben kockázatelemzésre azok esetleges korlátai miatt, illetve nem minden kockázatelemzési eljárás alkalmazható teljes értékű eseménymodellként.

A baleseti vagy eseménymodelleket Erik Hollnagel[1] az alábbi felosztásban kezeli:

- lineáris (esemény)modell, azon belül egyszerű lineáris és összetett (komplex) lineáris (esemény)modell;
- komplex nemlineáris (esemény)modell [13, p. 3].

Az egyszerű lineáris modellek azt feltételezik, hogy a baleset olyan események vagy körülmények sorozatának eredménye, amelyek egymás után hatnak egymásra, és – ahogy azt már az előző cikkben megfogalmaztam – így a balesetek megelőzhetők az aktuális eseménysorozat egyik okának kiküszöbölésével. Egyszerű lineáris modellek közé tartozik a hibafa- vagy az eseményfamodell is.

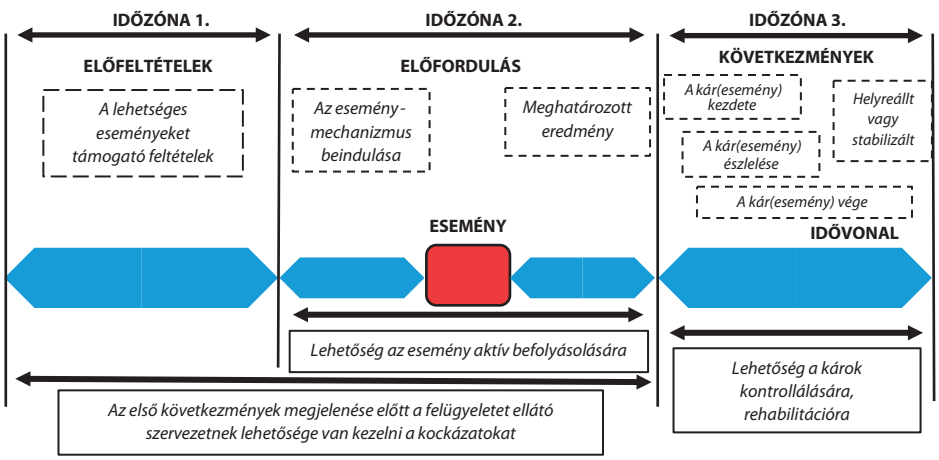
Az összetett (komplex) lineáris (esemény)modellek között is többféle irányvonal létezik. Ami nagyjából mindegyikre igaz, hogy az összetett lineáris modellek azon a feltételezésen alapulnak, hogy a balesetek a rendszeren belüli nem biztonságos cselekedetek, hibák és látens körülmények kombinációjának eredményei, amelyek lineáris utat követnek. A balesettől legtávolabbi tényezőket a szervezet vagy a környezet tevékenységeinek, míg a közvetlen kiváltó okokat a balesethez legközelebbi emberi kölcsönhatásoknak, hibáknak tulajdonítják. Ezek az egyszerű lineáris modellekből kifejlesztett kockázatelemzési, illetve baleset-megelőzési módszerek a kiváltó okok megtalálására és megszüntetésére, illetve az okokat elzáró biztonsági akadályok/korlátok felállítására összpontosítanak. Az 1970-es évektől a technológiai szint bonyolultabbá válása mellett a lineáris és az összetett lineáris modellek párhuzamosan fejlődtek. Ebben az evolúciós időszakban kifejlesztett kulcsfontosságú összetett lineáris modellek közé tartoznak *az energiakárosodási modellek,*[2] az *időbeli sorrendmodellek,*[3] a *járványtani modellek*[4] és a *rendszerszintű modellek*[5] [13, p. 7].

Az összetett lineáris modellek közül a *energiakárosodási modellekben* a veszélyforrás egy potenciálisan károsító energia, és a veszélyforrást szabályozó mechanizmus meghibásodása következtében ezen energia kontrollálásának elvesztése balesetet, sérülést vagy kárt okozhat. Ezek a mechanizmusok magukban foglalhatják a fizikai vagy szerkezeti elszigetelést, biztonsági akadályokat, folyamatokat és működési eljárásokat. Derek Viner[6] 1991-ben publikált könyvében úgy fogalmazott, hogy „a károsodás (sérülés) olyan beeső energia eredménye, amelynek intenzitása a befogadóval való érintkezés helyén meghaladja a befogadó károsodási küszöbértékét" [1, p. 42]. Ennek megfelelően az általa leírt modellben a veszélyforrást

[1] Erik Hollnagel pszichológus, egyetemi tanár, professor emeritus, PhD, Dél-dániai Egyetem, Dánia, Linköpingi Egyetem, Svédország.
[2] Energy Damage Model.
[3] Time Sequence Model.
[4] Epidemiological Model.
[5] System Level Model.
[6] Derek Viner biztonsági mérnök, egyetemi docens, CQ Egyetem, Ausztrália és Swinburne Egyetem, Ausztrália.

és a befogadót összeköti a térátviteli mechanizmus, vagyis az az eszköz, amellyel az energia és a befogadó összeér, feltételezve, hogy kezdetben távol vannak egymástól. A befogadó határa az a felület, amely az energiának kitett és az energiára érzékeny [13. pp. 7–8].

Az *időbeli sorrendmodellek* esetében az események időben egymást követve lépnek fel, egyrészt okozva az eseményt önmagát, másrészt az időben megjelenítve a következményeket. Ez a modell négy alapvető tulajdonságában tér el a lineáris eseménymodellektől. Az első ilyen tulajdonság a baleset kezdet- és végállapota meghatározásának szükségessége; a második a megtörtént események szekvenciális idővonalon történő ábrázolásának szükségessége; a harmadik a releváns tényezők feltárására szolgáló strukturált módszer szükségessége; a negyedik az események és körülmények meghatározására szolgáló grafikonkészítési módszer alkalmazásának szükségessége [13, p. 8]. Az események itt nem egy láncon vagy logikai kapukon felfűzött történések/okok sorozataként jelennek meg, hanem egy külön időzónákra szakaszolt idővonalon ábrázoljuk őket.



1. ábra
Időbeli sorrendmodell (a szerző [13, p. 9] alapján)

Viner úgy véli, hogy az esemény-következmény lineáris sorrendben történő események elemzéséhez az időbeli sorrendmodell által biztosított struktúra felhívja a figyelmet azon ellenintézkedésekre, amelyek egyébként nem feltétlenül lennének nyilvánvalók. Az 1. ábrán látható 1. időzónában lehetőség van az esemény bekövetkezésének megakadályozására, amennyiben az esemény kezdeményezése és az esemény bekövetkezése között rendelkezésre áll megfelelő hosszúságú idő. A 2. időzóna figyelmeztet az eseménymechanizmus közelgő bekövetkezésére, és lehetőséget biztosít az esemény bekövetkezésének valószínűségét csökkentő lépések megtételére, míg a 3. időzónában lehetőség van a kimenet és a bekövetkezett esemény okozta károk mérséklésére, csökkentésére, adott esetben a következmények rehabilitációjára [13, p. 9].

A *járványtani baleseti modellhez* illeszkedő baleset-megelőzési módszerek a teljesítménybeli eltérésekre és a baleset látens okainak megértésére összpontosítanak. A korábbi modellektől eltérően a fókuszpontot a szervezetben lévő rejtett okok vagy körülmények

megértésére helyezi át. Ezen rejtett körülmények általában az eljárásrendektől való eltérésekben vagy a nem biztonságos cselekedetekben nyilvánulhatnak meg, és ezek megszűnése vagy megszüntetése megakadályozhatja a baleset megismétlődését [13, p. 11].

Ezen epidemiológiai modellek egyik jó példája a James T. Reason[7]-féle svájcisajt-modell, amely Hollnagel megítélése szerint a rendszerben megbúvó járványtani hatásmechanizmusra építő komplex lineáris modell. A balesetet a szervezet működésében vírusként lappangó, adott körülmény vagy cselekmény hatására aktiválódó rejtett körülmények és a végrehajtó által elkövetett kockázatos cselekmények (emberi hibák és normasértések) lineáris kombinációjának tulajdonítja. Reason a nem kívánt események elemzésének fő irányát az egyénről a szervezetre és annak vezetésére helyezte át, ugyanakkor a megelőzési tevékenység lehetőségeit az egyén elítélése, a hibáztatás, és szankció alkalmazása helyett továbbra is a rendszer védelmének megerősítésében látta [4], [13, p. 10], [8, p. 8].

Általánosságban elmondható, hogy a balesetek során elkövetett hibákat és az eltéréseket általában az adott terület felügyeletét ellátó (munkavédelmi, légi közlekedési és/vagy munkaügyi) hatóságok negatív kontextusban látják, természetüknél, illetve keletkezésük, létrehozásuk jogi gyökerei miatt szabálykövetési igénnyel lépnek fel, és a hibákat szankcionálandó területként fogják fel. A hatóságok által a rendszer védelmének érdekében kezdeményezett egyes programok, mint például a biztonságos viselkedést ösztönző oktatások, azt próbálják elérni, hogy a tevékenységekre vonatkozó szigorú szabályokat és eljárásokat a végrehajtó személyek, illetve az üzemeltető és az üzembentartó szervezetek mindig kövessék. Ugyanakkor a kockázat csökkentő, eseménymegelőzési, biztonságos működést előtérbe helyező gondolkodás egyre inkább annak megértése felé halad, hogy miként lehet olyan megfelelően rugalmas működésű rendszert létrehozni, amely negatív következmények nélkül ellenáll az esetleges eltéréseknek vagy a szokatlan cselekedeteknek [13, p. 11].

Az 1980-as években egyes kutatók[8] a valóságban végbement baleseti események vizsgálata során úgy találták, hogy a nem kívánt események bekövetkezése nem lineáris, ennek következtében szükség van olyan modellekre, amelyek a balesetek leírásánál azok komplexitását is tükrözik, azaz „egy reális baleseti modellnek fel kell tudnia mutatni az események szekvenciális és egyidejű, nemlineáris lefolyását, és tükröznie kell az események időbeli kölcsönhatásait" [13, p. 11]. Az erre irányuló kutatói munka egyik eredménye a *rendszerszintű modellek* megjelenése. Hollnagel szerint a rendszerszintű modellek alaptétele, hogy a balesetek fő okozói a rendszerhibák, és nem csak az emberi mulasztás [4]; ennek következtében a kutatók elkezdtek foglalkozni néhány olyan iránnyal (ide nem értve a nemlineáris koncepciókat), amely megmutatta, hogy az események nem történnek elszigetelten attól a rendszerszintű környezettől, amelyben bekövetkeznek.

A terület egyik kutatója, Jens Rasmussen[9] a balesetek elemzése során részletesen foglalkozott az ok-okozati összefüggés problematikájával, és a közvetlen ok-okozati összefüggés, az idővonal és a baleseti modellezés közötti kapcsolat leírásához a filozófiából vett át fogalmakat. Rasmussen azt vizsgálta, hogy a valós világ eseményeit és tárgyait fel lehet-e bontani részletekre, és a tényleges okozati rendszerüket meg lehet-e magyarázni a baleset bekövetkezésére utaló ok-okozati összefüggések útján, ahol a korábbi események vagy cselekmények

[7] James T. Reason pszichológus, a Brit Birodalom lovagja, a Manchesteri Egyetem korábbi professzora, Anglia.
[8] Többek között Ludwig Benner, Jens Rasmussen és James T. Reason.
[9] Jens Rasmussen (1926–2018) rendszerbiztonsági és emberi tényező kutató, Risø Nemzeti Laboratórium, Dánia.

lappangó hatásai is szunnyadnak. Rasmussen felismerte, hogy a társadalmi-technikai rendszerek egyszerre összetettek és instabilak. Véleménye szerint az események lefolyásának tárgyalására tett kísérletek nem veszik figyelembe, hogy „az események és feltételek közötti kölcsönhatás zárt hurkai az egyéni és szervezeti alkalmazkodás magasabb szintjét jelentik […] a balesetelemzés által talált ok-okozati fa csak egy múltbeli eset feljegyzése", nem pedig az érintett esemény tényleges „kapcsolati struktúra modellje" [7, p. 454].

3. A komplex nemlineáris modellek megjelenése

A balesetek modellezésével kapcsolatos gondolkodás *a rendszerszintű modellek* megjelenése után tovább fejlődött, mivel egyes kutatások szerint a balesetek úgy tekinthetők, mint a valós környezetben előforduló, kölcsönhatásban lévő változók kombinációinak eredménye, és csak e több tényező kombinációjának és kölcsönhatásának megértése révén lehet a baleseteket valóban megérteni és megelőzni [13, pp. 3–4].

Ennek eredményeként az 1980–1990-es években megjelentek a komplex nemlineáris eseménymodellek, és kifejlesztésük bizonyos szempontból párhuzamosan zajlott az egyszerű lineáris, komplex lineáris eseménymodellek alkalmazásával, fejlődésével együtt. A 2000-es évek elejére két nagy komplex nemlineáris eseménymodell született meg. Az egyik a Hollnagel-féle funkcionális rezonancia baleseti modell[10] (FRAM), a másik a Nancy G. Leveson[11] által kidolgozott rendszerelméleti baleseti modell és folyamatelemzés[12] (STAMP).

A cikk elsősorban ezen modellek bemutatására és az azokra alapuló kockázatelemzési eljárások ismertetésére törekszik.

4. A FRAM-módszer ismertetése

Erik Hollnagel tanulmányozta a baleseti eseménymodellek, az ok-okozati összefüggések és az esemény bekövetkezését befolyásoló tényezőket, amelyek során az emberi/kognitív megbízhatóságot és az ember-gép interfészt vizsgálva eljutott oda, hogy az emberi munkavégzés, illetve tevékenység jelenléte mellett kialakított, rendkívül összetett és szorosan összekapcsolt társadalmi-technikai rendszerek vizsgálatában bevezette a balesetek háromdimenziós gondolkodásmódjának koncepcióját. Megállapításai szerint ezen rendszermodelleket szorosan összekapcsoltnak kell tekinteni, és ennek megfelelően kell vizsgálni. Elgondolása szerint a szervezetek biztonsági céljait pedig úgy kell meghatározni, hogy azok a korlátok és védekező mechanizmusok felállítása helyett inkább olyan rendszerekre összpontosítsanak, amelyek képesek az eltérések nyomon követésére és ellenőrzésére, valamint lehetővé tegyék, hogy a rendszerek (emberi) hibatűrők legyenek [13, p. 17].

A FRAM a komplex rendszerszintű balesetek elméletén alapul, ugyanakkor abból az alapkoncepcióból indul ki, hogy a rendszer eltérései és tűréshatárai akkor vezetnek balesethez, ha a rendszer normál üzemmódban nem képes elviselni az ilyen eltéréseket. A biztonsági

[10] Functional Resonance Accident Model.
[11] Nancy G. Leveson professzor, rendszer- és szoftverbiztonsági kutató, egyetemi tanár, Massachusettsi Műszaki Egyetem, Cambridge, Amerikai Egyesült Államok.
[12] System-Theory Accident Model and Process.

rendszerek/alrendszerek működési eltéréseit a szakemberek a legtöbb alkalmazott rendszer esetében normálisnak tekintik, ugyanakkor ezen eltérések azok, amelyek reprezentálják az összetett rendszerek működéséhez szükséges változó teljesítményt, beleértve a tervezés korlátait, a technológia tökéletlenségeit, a munkakörülményeket és a bemenetek olyan kombinációit, amelyek általában lehetővé tették a rendszer működését. Az emberek és a társadalmi rendszerek, amelyekben tevékenykednek, szintén a rendszer változékonyságát képviselik, különös tekintettel arra, hogy az embereknek alkalmazkodniuk kell, és kezelniük kell az idővel és a hatékonysággal kapcsolatos követelményeket is [4, p. 168].

4.1. A kockázatkezelés társadalmi-technikai megközelítése

Hollnagel elmélete alapvetően abban különbözik a korábban kialakított modellektől, hogy szerinte a társadalmi-technikai rendszerek biztonsága és a rendszerekben fellépő kockázatok megértése nem konzervatív megközelítéssel, hanem attól eltérő úton érhető el. Véleménye szerint a kockázatértékelés bevett megközelítési módszerei mind megkövetelik, hogy a rendszert részletesen le lehessen írni, például egy sor forgatókönyvre és a megfelelő szükséges funkcióra való hivatkozással. Más szóval, a rendszernek követhetőnek kell lennie [3, p. 14].

Álláspontja szerint társadalmi-technikai rendszerek, ideértve például az atomerőműveket vagy a magas integráltsági fokú légi közlekedési rendszereket, repülőgépeket is, általában nehezen kezelhetők. Ez azt jelenti, hogy a bevált módszerek nem feltétlenül alkalmasak esetükben. Az sem megfelelő megoldás, hogy a rendszerleírásokat annyira leegyszerűsítsék, hogy azok a gyakorlatban követhetővé váljanak. Ezért olyan megközelítéseket kell keresni, amelyek a nehezen kezelhető rendszerek, azaz a hiányos vagy alulspecifikált rendszerek esetében is alkalmazhatók [3, p. 14]. Hollnagel álláspontja szerint az ellenálló képességre fókuszáló mérnöki tevékenység (Resilience Engineering), a rendszerek rugalmas és ellenálló tervezése – a társadalmi-technikai rendszerszemléleten belül – egy ilyen megközelítést képvisel.

A kockázat és a biztonság hagyományos megközelítései a „hibák" számbavétele és a meghibásodási valószínűségek kiszámítása érdekében a rendszerek felépítésének és folyamatainak részletes leírásától függenek. A rugalmas, ellenálló tervezés helyett a jellemző folyamatok, funkciók leírásából indul ki, és azt keresi, hogyan lehet javítani a szervezet azon képességét, hogy megfelelően robusztus, de rugalmas folyamatokat hozzon létre. Emellett miként lehet megvalósítani azt, hogy a szervezet önmaga figyelemmel kísérje és felülvizsgálja a kockázati modelleket, és hogy proaktívan használja az erőforrásokat a váratlan fejleményekkel vagy a folyamatos termelési és gazdasági nyomással szemben [3, pp. 14–15].

A FRAM-módszer megértéséhez és alkalmazásához figyelembe kell venni a Hollnagel által kidolgozott, a társadalmi-technikai rendszerekre vonatkozó alapelveket:

1. alapelv: A siker és a kudarcok egyenértékűsége. A bonyolult rendszerekben a teljesítményfeltételek mindig alulméretezettek, specifikáltak, például sohasem áll annyi erőforrás rendelkezésre, mint amennyire számítunk. Mivel egy folyamat, rendszer működése során elvégzett munkateljesítményt nem lehet minden részletre kiterjedően meghatározni, az egyéneknek és a szervezeteknek mindig az aktuális feltételekhez kell igazítaniuk teljesítményüket. Mivel az erőforrások és az idő végesek, a teljesítmény ilyen kiigazításai menthetetlenül közelítő jellegűek lesznek, ebből kifolyólag a teljesítmény változékonysága elkerülhetetlen, ami egyben a siker és a kudarc forrása is [3, p. 15]. Ezekből kifolyólag a siker így annak a következménye, hogy

a csoportok, egyének és szervezetek képesek előre látni a kockázat változékonyságát, mielőtt a kár bekövetkezik; a kudarc pedig egyszerűen ennek átmeneti vagy tartós hiánya [3, p. 44].

2. alapelv: A „közelítő kiigazítások" elkerülhetetlenség. Sok kedvezőtlen esemény az alkatrészek és a rendszer normál funkcióinak meghibásodására vagy hibás működésére vezethető vissza, ellenben nagyon sok esemény nem ezek miatt következik be. Az ilyen nehezen kezelhető események leginkább úgy értelmezhetők, mint a normál teljesítményváltozékonyság váratlan kombinációinak eredménye. A nemkívánatos eseményekre ezért úgy szükséges tekinteni, mint a valós világ komplexitásával való megbirkózáshoz szükséges alkalmazkodási képesség fordítottja [3, p. 15].

Ebben a szemléletben a rendszer normális működésének változékonysága két alapvető tényből fakad. Ahogy a korábbi elvnél megfogalmaztam, egyrészt a működési feltételek általában alulméretezettek, ezért ritkán vagy soha nem úgy vannak biztosítva, mint ahogyan azt eltervezték vagy előírták.[13] Ez azt jelenti, hogy a gyakorlatban lehetetlen előre olyan részletes utasításokat készíteni, amelyeket pontosan be lehet tartani. A megoldás ehelyett az, hogy olyan iránymutatásokat és eljárásokat adunk meg, amelyek a konkrét cselekvések alapjául szolgálhatnak. Az iránymutatásokat és az eljárásokat általában széles körű szakmai képzéssel szükséges támogatni.

Másrészt a működési feltételek dinamikusan, többé-kevésbé szabályozott módon változnak. A változó körülmények miatt azon személyeknek, akiknek egy adott helyzetben cselekedniük kell, legyenek akár vezetők, akár üzemeltetők, csak rövid távra tudnak biztonsággal tervezni. Emiatt folyamatosan készen kell állniuk arra, hogy terveiket felülvizsgálják, és a tervek végrehajtását az aktuális körülményekhez igazítsák. Ez a változékonyság nemcsak a rendszer pillanatnyi működését jellemzi, hanem a rendszer teljes élettartama alatt – az életciklus kezdetétől a végéig – fennáll. Ahhoz, hogy az emberek bármit el tudjanak végezni, mindig az aktuális körülményekhez kell igazítaniuk teljesítményüket. Az ember mint entitás szerencsére képes arra, hogy hatékony módszereket találjon a munkahelyi problémák leküzdésére, és ez a képesség döntő fontosságú a biztonság szempontjából is. Amennyiben az emberek váratlan események esetén mindig mereven követnék a szabályokat és az eljárásokat, sokkal több baleset és incidens lenne. Az emberi teljesítmény tehát egyszerre növelheti és csökkentheti a rendszer biztonságát. A rendszer értékelési módszereinek képesnek kell lenni e kettősség kezelésére [3, p. 45].

3. alapelv: A következmények kialakulnak. A hatékony biztonságirányítás nem alapulhat utólagos mérlegelésen, és nem támaszkodhat hibatáblázatokra és a meghibásodási valószínűségek kiszámítására. Az irányításelmélet általános tézise, hogy a hatékony irányítás nem hagyatkozhat kizárólag a visszacsatolásra, kivéve a nagyon egyszerű rendszereket. A hatékony irányítás megköveteli, hogy a válaszokat adott esetben előre elkészítsék, és néha idő előtt végrehajtsák azokat, azaz *feedforward*ot (előrecsatolást) alkalmazzanak. Ezért nem elegendő, ha a biztonságirányítást a kedvezőtlen kimenetek számbavételére alapozzuk, mivel ezek diszkrét események, amelyek kizárják a rendszer dinamikáját [3, p. 15].

A normál teljesítmény változékonysága önmagában ritkán elég nagy ahhoz, hogy baleset okozója legyen, vagy akár üzemzavarnak minősüljön. Több funkció változékonysága azonban váratlan módon kombinálódhat – funkcionális rezonancia lép fel –, ami aránytalanul nagy következményekhez vezethet, és így nemlineáris hatásokat eredményezhet. Mind a meghibásodások,

[13] Ez a társadalmi-technikai rendszerek megoldhatatlanságának következménye [3, p. 45].

mind a normális teljesítmény inkább „felbukkanó tulajdonság",[14] mint eredő jelenség, mivel egyik sem magyarázható kizárólag bizonyos alkatrészek vagy részek funkcióira vagy meghibásodásaira való hivatkozással, vagy nem tulajdonítható annak. A társadalmi-technikai rendszerek nehezen kezelhetők, mert a körülményekre és az igényekre reagálva változnak és fejlődnek. Ezért lehetetlen leírni a rendszer összes kapcsolódási pontját, és lehetetlen a legszabályosabb eseményeknél többet előre jelezni [3, p. 46].

4. alapelv: Funkcionális rezonancia. Rendszerszemléletű megközelítésként a FRAM leküzdi a bevett módszerek belső korlátait azáltal, hogy a rendszerfunkciók közötti kapcsolatokra összpontosít. A FRAM a hagyományos ok-okozati összefüggést is a rezonancia elvével helyettesíti. Ez azt jelenti, hogy több funkció változékonysága időről időre rezonálhat, abban az értelemben, hogy egymást erősíthetik, és ezáltal az egyik funkció változékonysága meghaladhatja a normális határokat.[15] A következmények inkább szoros kapcsolódásokon keresztül terjedhetnek, mint azonosítható és megszámlálható ok-okozati kapcsolatokon keresztül. A rezonancia analógia hangsúlyozza, hogy ez egy dinamikus jelenség, tehát nem az oksági kapcsolatok egyszerű kombinációjának tulajdonítható. Ez az elv lehetővé teszi a rendszerműködés jellegzetes dinamikájának megragadását, tehát olyan „felbukkanó" rendszertulajdonságok azonosítását, amelyek nem érthetők meg, még akkor sem, ha a rendszert izolált összetevőkre bontjuk [3, p. 47].

A fentiek mellett fontos kiemelni, hogy Reasonhoz hasonlóan úgy ítéli meg, hogy a biztonságot nem lehet elszigetelten kezelni az alapvető (például üzleti, működési) folyamatoktól, és ez fordítva is igaz. A biztonság a termelékenység előfeltétele, a termelékenység pedig a biztonságé. A biztonságot inkább fejlesztésekkel érjük el, nem pedig korlátozásokkal [3, p. 15].

4.2. A társadalmi-technikai rendszerek biztonsága

Hollnagel szerint a társadalmi-technikai komplex rendszerek biztonsága négy alapvető feltételtől függ:

1. A rendszer vagy szervezet képes-e a rendszeres és szabálytalan fenyegetésekre robusztus, ugyanakkor rugalmas módon reagálni.
   Egyetlen rendszer sem maradhat fenn anélkül, hogy ne tudna valahogy reagálni, ha valami rosszul sül el. Valójában ez a reaktív biztonságirányítás lényege. Sok rendszer azonban csak korlátozottan képes, vagy éppen nem képes a váratlan igényekhez igazítani a reakcióit.
2. A rendszer vagy szervezet rugalmasan képes-e nyomon követni, hogy mi történik, beleértve a saját teljesítményét is.
   Erre a tulajdonságra minden olyan rendszer esetében szükség van, amely dinamikus és kiszámíthatatlan környezetben létezik. Magának a nyomon követésnek továbbá

[14] A szakirodalom által *Emergent Property*nek nevezett, olyan (biztonsági) rendszertulajdonságok, amelyek nem az egyes összetevők összegzésében jelennek meg, hanem az összetevők kölcsönhatásakor „keletkeznek". A „felbukkanó" tulajdonságok csak akkor kezelhetők megfelelően, ha figyelembe vesszük valamennyi technikai és társadalmi aspektusukat [9, p. 10].

[15] Az eredmény természetesen lehet előnyös és hátrányos is, habár a természetes okok miatti biztonság tanulmányozása az utóbbira összpontosít.

nyitottnak kell lennie a kritikai értékelésre, hogy a rendszer ne hagyatkozzon olyan bevett gyakorlatokra, amelyek már nem feltétlenül megfelelők.

3. A rendszer vagy szervezet hosszabb távon előre látja-e a kockázatokat és a lehetőségeket.
   A lehetséges események előrejelzésének túl kell mutatnia a klasszikus kockázatértékelésen, és nemcsak az egyes eseményeket kell figyelembe vennie, hanem azt is, hogy azok hogyan kombinálódhatnak és hogyan befolyásolhatják egymást. Míg sok rendszernél van valamilyen mértékű nyomon követés, csak kevés esetben tesznek jelentős erőfeszítéseket az előrejelzésre, legalábbis ami a biztonságot illeti.
4. A rendszer vagy szervezet képes-e a tapasztalatokból tanulni.
   A tanuláshoz többre van szükség, mint a balesetek, incidensek és balesetközeli esetek adatainak gyűjtésére, vagy egy vállalati szintű adatbázis létrehozására. Míg az adatok viszonylag könnyen és többé-kevésbé rutinszerűen vagy eljárásszerűen összegyűjthetők, addig a tapasztalatok feldolgozása általában folyamatos, jelentős erőfeszítéseket és időt igényel [3, p. 16].

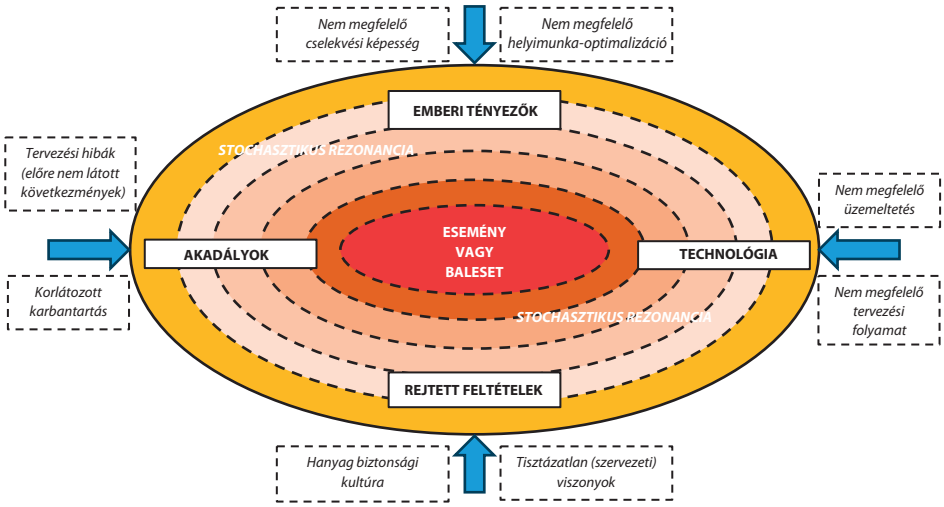
Mind a négy tulajdonság döntően attól függ, hogy a szervezet milyen modellel rendelkezik önmagáról, azaz arról, hogyan látja saját magát és mit csinál, valamint arról a környezetről, amelyben létezik. A kialakított modell szempontjából a szervezetben és a szervezet körül zajló folyamatok természetére vonatkozó feltételezések, az oksági kapcsolatok nagy jelentőséggel bírnak. Ez a modell, illetve ezek a feltételek különösen fontosak a balesetek kivizsgálása és a kockázatértékelés szempontjából, mivel alapvetően meghatározzák, hogy mit vesznek figyelembe az elkészítése során, és hogyan írhatók le a rendszer összetevői közötti kapcsolatok [3, p. 17].

4.3. A FRAM alapjai

Hollnagel felismerte, hogy az összetett (társadalmi-technikai) rendszerek nagyszámú alrendszerből és komponensből állnak, és a teljesítményváltozások rendszerint elnyelődnek a rendszeren belül, kevés negatív hatással az egész működésére. A teljesítményváltozékonyság négy fő forrását azonosította:

1. emberek – az emberi teljesítőképesség variabilitása;
2. technológia – a technológiában rejlő problémák, meghibásodások;
3. látens feltételek (rejtett körülmények);
4. akadályok (védelmi vonalak) – hiányzó vagy nem megfelelő védelmi vonalak.

Hollnagel elgondolása szerint amikor a rendszeren belüli változók túl nagyok lesznek ahhoz, hogy a rendszer elnyelje őket; esetleg az emberek, a technológia, a rejtett körülmények és a védelmi vonalak, ezen alrendszeri változók kombinációja révén az eredmény nem észlelhető, és a rendszer működésében nem kívánt eredmények keletkeznek, vagyis „funkcionális rezonancia" lép fel, akkor a rendszer nem tud megbirkózni a normál működési módjával, illetve végső soron a normál működést megzavaró, attól eltérő üzemmódokkal.



2. ábra
A FRAM általános modellje (a szerző [13, p. 18] alapján)

Az 2. ábra azt mutatja meg, hogy a változékonyság négy forrása különböző mértékben hathat egy rendszer működésére, amely a behatásokat igyekszik elnyelni, addig a pontig, amikor az egyes hatások által a rendszerben keltett sztochasztikus rezonancia eredményeként bekövetkezik az esemény vagy a baleset.

A FRAM végrehajtása emellett azt is bemutatja, hogy egy szervezeten belül a különböző funkciók hogyan kapcsolódnak más funkciókhoz. Külön hangsúlyt kap az egyes funkciók változékonyságának megértése, és hogy ez a változékonyság hogyan kezelhető [4, p. 171].

4.4. A FRAM által leírt folyamatok aspektusai

A FRAM a rendszerhibákat (káros eseményeket) a normál teljesítmény változékonyságából eredő funkcionális rezonancia eredményeként írja le. A módszer az egyéni és/vagy szervezeti funkciók modelljére vagy ábrázolására utal, ahol az egyes funkciók jellemzői adják az alapot a potenciális változékonyság leírásához. A rezonancia elvére hivatkozva magyarázható meg, hogy a kis vagy akár a jelentéktelen eltérésekből hogyan keletkezhetnek aránytalanul nagy hatások.[16] A hangsúly inkább a dinamikus függőségeken van, mint a meghibásodási valószínűségeken. A funkciók/folyamatok közötti kapcsolatokat hat függőségi viszony vagy szempont (bemenet, kimenet, idő, irányítás, előfeltételek és erőforrások) segítségével írjuk le, és ezek inkább potenciálisak, mint ténylegesek, azaz nincsenek előre meghatározott ok-okozati kapcsolatok [3, p. 43]. A függőségi szempontok részletesebben kibontva az alábbiak:

[16] Hullámerősítés, interferencia.

1. *Bemenet.* A folyamat végrehajtásához szükséges anyag, energia, információ, amely elindítja magát a cselekvést, vagy átalakul a *Kimeneten* megjelenő „kimeneti eredménnyé". A FRAM szempontjából ugyanakkor bemenetnek számít akár egy olyan jel is, amely aktiválja, elindítja a folyamatot, azaz egy utasítás, parancs is annak tekinthető [2, p. 9].
2. *Kimenet.* A folyamat végrehajtásának eredményeként jön létre.[17] Emellett ugyanakkor a *Kimenet* akár a vizsgált rendszerben egy vagy több részfolyamat kimeneti paraméter állapotváltozását is leírhatja, így lehet például egy másik folyamat indításának jele is [2, p. 9].
3. *Előfeltételek.* Sok esetben előfordulhat, hogy egy funkciót vagy folyamatot nem lehet elindítani, amíg egy vagy több előfeltétel nem áll rendelkezésre. Ezek az előfeltételek olyan rendszerállapotokként értelmezhetők, amelyeket a folyamat végrehajtása előtt feltétlenül ellenőrizni kell. Az előfeltétel azonban önmagában nem jelenti a függvényt elindító jelet, azaz csak a *Bemenet* indíthatja el a folyamatot [2, pp. 9–10].
4. *Erőforrások.* Az erőforrás olyan dolog, amelyre egy folyamat végrehajtása során van szükség, vagy amelyet a folyamat végrehajtásához felhasználunk. Az erőforrás lehet anyag, energia, információ, szakértelem, szoftver, eszköz, munkaerő stb. Mivel az egyes erőforrások a folyamat végrehajtása során elfogynak, mások pedig nem, célszerű különbséget tenni egyrészt a *(megfelelő) erőforrások,* másrészt a *végrehajtási feltételek* között. Egy (megfelelő) erőforrást egy folyamat fogyaszt el, annak mennyisége idővel csökken, ezért meg kell újítani vagy pótolni kell. Egy végrehajtási feltételnek csak akkor kell rendelkezésre állnia vagy léteznie, amikor egy folyamat aktív, de nem fogy el, mint egy (megfelelő) erőforrás. Az *Előfeltétel* és a végrehajtási feltétel között az a különbség, hogy az előbbire csak a folyamat elindítása előtt van szükség, nem a végrehajtása közben [2, p. 10].
5. *Irányítás.* Az irányítás az, ami úgy felügyeli vagy szabályozza a folyamatot, hogy az a kívánt kimeneti eredményt produkálja. Az irányítás lehet egy terv, ütemterv, eljárás, illetve irányelvek vagy utasítások összessége, egy program (algoritmus) stb. Az irányítás másik, kevésbé formális típusa a társadalmi kontroll vagy a munka elvégzésének módjára vonatkozó elvárások. A társadalmi kontroll lehet külső, például mások (vezetőség, szervezet, munkatársak) elvárásai, amelyek néha kifejezetten erősen befolyásolhatják a végrehajtást, és lehet belső is, például amikor megtervezünk egy munkát, és mentálisan végiggondoljuk, hogy mit, mikor és hogyan kell elvégezni, vagy amikor azt gondoljuk át, hogy mások mit várnak el tőlünk egy folyamat végrehajtása során [2, p. 10].
6. *Idő.* Az idő több szempontból befolyásolhatja egy folyamat vagy funkció végrehajtását. Az idő vagy inkább az időbeli viszonyok az *Irányítás* egyik formájának is tekinthetők, mint amikor az idő két vagy több cselekvés sorrendjét (szekvenciafeltételek) jelenti.[18] Az idő vonatkozhat önmagában egy folyamatra is, akár az óraidőhöz, akár az eltelt időhöz viszonyítva. Az időt értelmezhetjük *Erőforrásként*[19]

[17] Például egy folyamat a Bemeneten beérkező adatok feldolgozásának eredményeként felhasználható információt biztosít a Kimeneten [2, p. 9].

[18] Egyes rendszerekben egy folyamatot például egy másik folyamat előtt, egy másik folyamat után vagy egy másik folyamattal átfedésben – párhuzamosan – kell végrehajtani (vagy befejezni) [2, p. 10].

[19] Például amikor valamit egy bizonyos időpont előtt vagy egy bizonyos időtartamon belül kell befejezni [2, p. 10].

vagy *Előfeltételként*[20] is. Mégis, ahelyett, hogy az *Időt* a másik három függőségi szempont egyikének részeként tartanánk számon, észszerű önálló aspektusként kezelni [2, pp. 10–11].

A függőségi szempontok segítségével meghatározható, hogy két folyamat vagy cselekvés a teljesítményfeltételek függvényében összekapcsolható-e egymással. Ily módon lehetőség nyílik a szándékolt és a nem szándékolt csatolások azonosítására. A balesetvizsgálat esetén ez arra használható, hogy megtaláljuk, hol keletkezhettek egybeesések, amelyek negatívan befolyásolták a normál működést; kockázatértékelés esetén pedig arra, hogy megmagyarázzuk, hogyan keletkezhetnek egybeesések a teljesítmény változékonyságából, és így azonosítsuk a potenciális kockázatokat egy adott helyzetben [3, p. 43].

4.5. A FRAM-módszer lépései

Jelenlegi formájában a FRAM-módszer a következő öt lépésből áll:

1. Az *első lépés az elemzés céljának meghatározása*, mivel a FRAM-ot úgy fejlesztették ki, hogy mind a balesetek kivizsgálására (múltbeli események), mind a biztonság értékelésére (jövőbeli események) használható legyen.
2. A *második lépés a rendszerfunkciók (folyamatok) azonosítása és leírása*. Egy funkció (folyamat) a FRAM szempontjából olyan tevékenységet jelent, amely fontos vagy szükséges következményekkel jár egy másik tevékenység állapotára vagy tulajdonságaira nézve.
3. A *harmadik lépés az egyes egyedi funkciók (folyamatok) potenciális változékonyságának felmérése és értékelése*. A javasolt módszertan a folyamatok teljesítményének változékonyságát befolyásoló közös feltételek egy halmazának előzetes értékelését használja. A közös feltételek a Hollnagel által leírt közös teljesítményfeltételekből származnak. Ezt az értékelést össze kell vetni a baleseti adatbázisból kinyert retrospektív információkkal, amennyiben az adatok rendelkezésre állnak.
4. A *negyedik lépés a funkcionális rezonancia azonosítása*. E lépés célja annak meghatározása, hogy az egyik funkcióból származó változékonyság milyen módon terjedhet el a rendszerben, és hogyan kombinálódhat más funkciók változékonyságával. Funkcionális rezonancia esetén a változékonyság kombinációi olyan helyzeteket eredményezhetnek, amelyekben a rendszer elveszíti a változékonyság biztonságos kezelésére való képességét. A terjedés történhet közvetlenül egy funkció vagy folyamat kimenetén keresztül, és közvetve azon hatásokon keresztül, amelyeket a változékonyság a közös feltételekre gyakorolhat.
5. A FRAM elemzés *ötödik* és egyben utolsó *lépése a rendszerben bevezetendő hatékony ellenintézkedések azonosítása*. A FRAM tekintetében az ellenintézkedések célja a teljesítményváltozékonyság csillapítása a rendszer biztonságos állapotban tartása

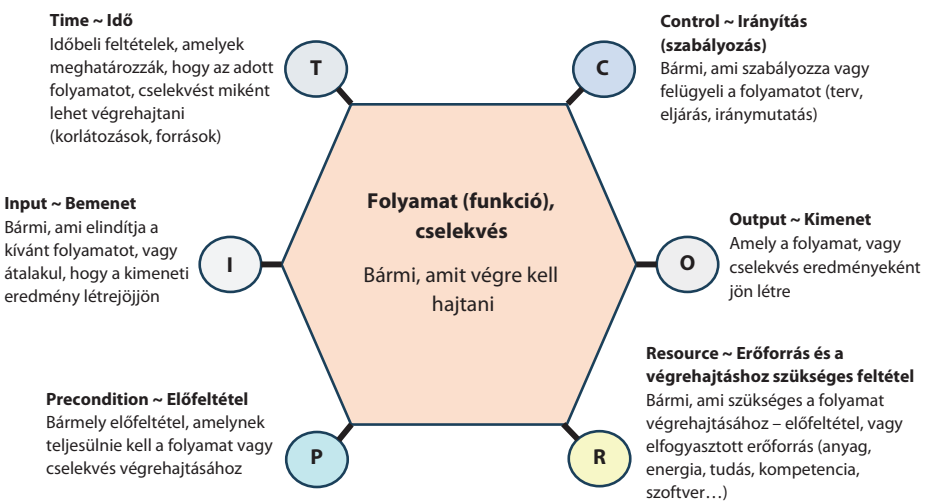
[20] Például úgy, hogy egy folyamat nem kezdődhet el egy bizonyos idő előtt, vagy hogy nem kezdődhet el egy másik folyamat befejezése előtt [2, p. 10].

érdekében. A rugalmas tervezés elvével azonban összhangban van, hogy olyan intézkedéseket is figyelembe kell venni, amelyek fenntarthatják vagy felerősíthetik a kívánt vagy jobb eredményekhez vezető funkcionális rezonanciát [3, p. 49].

4.6. A FRAM-módszer szemléltetése

A FRAM-módszerhez tartozik a fejlesztők honlapján[21] elérhető, a módszer ábrázolását elősegítő, az egyes események közötti kapcsolatokat láthatóvá tevő szoftver,[22] valamint egy másik, táblázatos formátumú, az egyes folyamatok megértését elősegítő alkalmazás.[23]

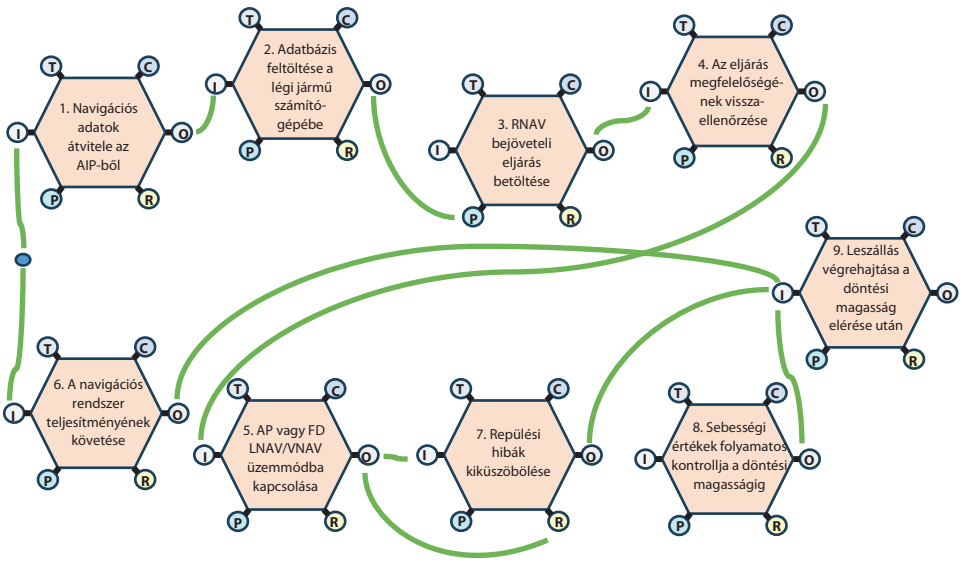
A FRAM-módszer a szemléltetés alapjaként egy hatszögletű alapábrát alkalmaz, amely mindig egy adott eseményt, cselekvés lépését tartalmazza (3. ábra). Az egyik funkció változékonysága más funkciók változékonyságát is befolyásolhatja. A hatszög csúcsai a FRAM – korábban már említett – függőségi viszonyai, aspektusai, amelyek egyben kapcsolódási pontként szolgálnak több esemény, cselekvés – mint további hatszögek – összekötéséhez. Ahogy korábban már leírtuk, a hatszög csúcsai olyan függőségi viszonyokat jelentenek, amelyek inkább potenciálisak, mint ténylegesek, azaz nincsenek előre meghatározott ok-okozati kapcsolatok. A függőségi kapcsolatok segítségével megjeleníthető, hogy a két cselekvés a teljesítményfeltételek függvényében összekapcsolható-e egymással [2, p. 11].



3. ábra
A FRAM alapeleme és a hat aspektusa (a szerző [2, p. 11] alapján)

[21] Lásd: https://functionalresonance.com/the-fram-model-visualiser/
[22] FRAM Model Visualiser (FMV).
[23] FRAM Model Interpreter (FMI) – 2019-től [4].

Erik Hollnagel és Örjan Goteman[24] közös cikkben [6] elemezte a FRAM alkalmazásával a területi navigációra épülő[25] (RNAV) bejöveteli eljárás végrehajtását. Anélkül, hogy ismertetnénk a 2004-es publikáció tartalmát és a bejöveteli eljárás részletes FRAM-elemzését, a 4. ábra leképezi az RNAV bejöveteli eljárás végrehajtását mint a „rendszer" normál állapotát a FRAM-modell alkalmazásával megjelenítve.

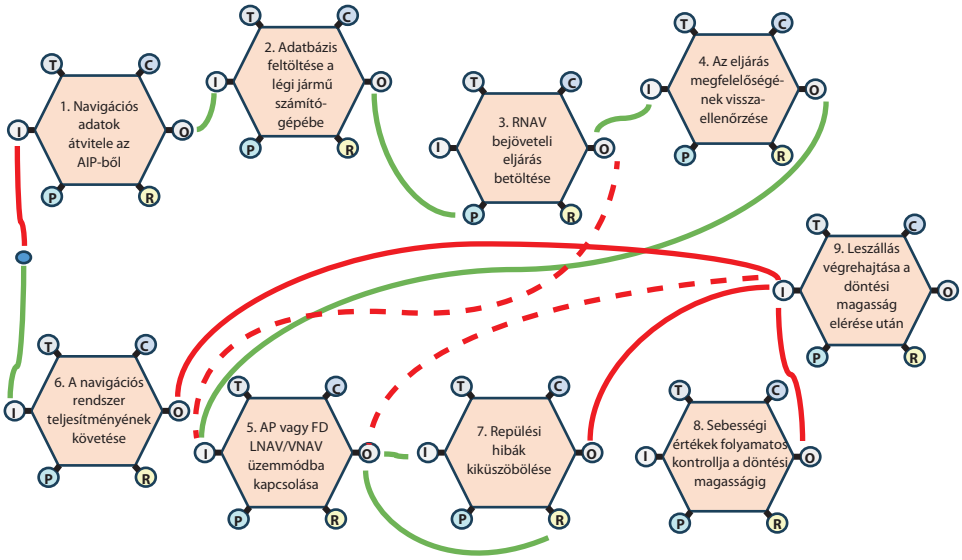


4. ábra
Az RNAV bejöveteli eljárás normál működési állapota (a szerző [6, p. 7] alapján)

A 4. ábrán kilenc lépésben (a folyamat összefűzésével) jelenik meg a vizsgált RNAV bejöveteli eljárás. A FRAM-elemzés során minden egyes folyamat esetében meg kell határozni annak leíró jellemzőit (mi kell az adott folyamat indításához, mennyi ideig fog működni, mi lesz a kimeneten stb.), majd ezek ismeretében kialakíthatók a folyamatok közötti kapcsolatok. A fő kapcsolatok alapvetően a kimenetek és a bemenetek között vannak, azonban egyes esetekben a kimenetek és az erőforrások között is megjelennek, ami azt jelenti, hogy az egyik folyamat kimenete egy másik folyamat számára erőforrás. A 4. ábra azt is megmutatja, hogy a függőségek nem a folyamatok egyszerű sorrendjét jelentik, hanem egy folyamatnak lehet kapcsolódása több folyamathoz is, mint ahogy több folyamat kapcsolódhat egy adott folyamathoz. Az RNAV bejöveteli eljárás megjelenítésénél a folyamatok kapcsolódása balról jobbra nézve időbeli kapcsolatot követ, ugyanakkor más esetekben ez nem feltétlenül van így, azaz – ahogy már korábban volt róla szó – az egyes folyamatok relatív pozíciója nem hordoz semmilyen jelentést [6, p. 7].

[24] Örjan Goteman, kereskedelmi pilóta, egyetemi tanár, Lund Egyetem, Svédország.

[25] Area Navigation (RNAV). Az RNAV egy olyan navigációs módszer, amely lehetővé teszi a légi jármű bármilyen kívánt repülési útvonalon történő üzemeltetését egy adott állomáshoz kötött *(stacioner)* navigációs segédeszközök lefedettségén belül, vagy önálló navigációs segédeszközök képességének határain belül, vagy ezek kombinációjával [5, p. 5].



5. ábra
Funkcionális rezonancia megjelenítése az RNAV bejöveteli eljárás esetén (a szerző [6, p. 8] alapján)

Az 5. ábra alapján látható, hogy az RNAV bejöveteli eljárás elemzése hol tárt fel funkcionális rezonanciát, azaz hogy hol mehet félre a „rendszer" normál működése (folytonos piros vonallal jelölve), illetve hol lehetnek potenciálisan olyan, esetlegesen hibás vagy nem meglévő kapcsolatok a folyamatok között, amelyeket előzetesen nem vettek számításba (szaggatott piros vonallal megjelölve).

Az 5. ábra megmutatja továbbá azt is, hogy az egyes folyamatok variabilitása mikor lép kölcsönhatásba vagy kombinálódik egymással, azaz láthatóvá válik, hogy egy adott funkciót, folyamatot esetleg helytelenül hajtanak végre, vagy akár el is hagynak. Amennyiben a nem megfelelő feltételek közül egyesek több funkcióhoz is kapcsolódnak, az a rendszer általános érzékenységére utalhat. A nagy teljesítményváltozékonyság ezért azt jelenti, hogy egyes bemenetek vagy előfeltételek kimaradnak (nem ellenőrzik megfelelően őket), és így a folyamatok között helytelen kapcsolódások fordulhatnak elő [6, p. 7].

4.7. A FRAM mint keretrendszer

Elmondása alapján Hollnagel nem azért alkotta meg a FRAM-et, hogy balesetelemzési módszer legyen [12, p. 1]. Álláspontja szerint ugyan a FRAM-et a századforduló környékén a biztonság általános értelmezésének összefüggésében fejlesztette ki, de nemcsak balesetelemzésre vagy biztonságirányításra, hanem feladatelemzésre, rendszertervezésre stb. is felhasználható. Azaz meglátása szerint a FRAM nem biztonsági eseménymodell, de nem is rendszermodell; inkább egy módszer, amely alapján egy (rendszer)modellt lehet felépíteni, és nem egy modell, amely egy módszer alapja.

Emellett a FRAM nem egy folyamatábrázolási eszköz, mivel az általa felépített modell általános grafikus ábrázolása megmutatja ugyan az elemeket (amelyek funkciókat, folyamatokat képviselnek) és a köztük lévő lehetséges kapcsolódásokat, de a cél a folyamatokban meglévő interdependenciák reprezentálása, és nem az, hogy bemutassa az elemek közötti – információ, anyag vagy energia – áramlását [2, p. 2], [12, p. 1].

5. A STAMP-modell alapjai

A FRAM-mel párhuzamosan kifejlesztett rendszerelméleti baleseti modell és folyamatok[26] (STAMP) egy olyan keretrendszert adnak meg, amelyet a balesetek megértésére és a (rendszer) biztonság javítására fejlesztettek ki. Az alapelméletet és a hozzá tartozó gyakorlati eljárásrendet az Egyesült Államokban, Bostonban (Cambridge), a Massachusettsi Műszaki Egyetem[27] kutatója, Nancy G. Leveson és kollégái alakították ki [9]. A STAMP a rendszerelmélet által meghatározott elgondolások alapján működik, a rendszer különböző elemei közötti interakciók vizsgálatával holisztikus megközelítést kínál a balesetek elemzéséhez.

A modell kidolgozására Leveson véleménye szerint elsősorban azért volt szükség, mert a korábbi eseménymodellek az ok-okozati összefüggések korlátozott vizsgálatára ösztönöznek – általában a lineáris oksági kapcsolatokat hangsúlyozzák –, és ilyen esetekben nehéz beépíteni az egyes szervezetrendszerekben meglévő nemlineáris kapcsolatokat, ideértve a visszacsatolásokat is. A bonyolult, összetett rendszerekben bekövetkezett események közelmúltbeli vizsgálata során kiderült számára, hogy a balesetek bekövetkezésének legfontosabb tényezője a vezetőség biztonság iránti elkötelezettsége és a szervezet vagy az iparág alapvető biztonsági kultúrája volt [9, p. 240]. Ennek megállapításához ugyanakkor olyan összefüggéseket is fel kellett tárni, amelyek a korábbi modellek alkalmazásával nem feltétlenül voltak egyértelműek.

Leveson szerint a hagyományos eseménymodellekben az azonosított ok-okozati tényezők a figyelembe vett eseményektől és az ezekhez az eseményekhez kapcsolódó feltételek kiválasztásától függenek. A veszteséget közvetlenül megelőző vagy abban közvetlenül érintett fizikai eseményektől eltekintve azonban az elemzés során vizsgált (rész)események kiválasztása szubjektív, az ezeket magyarázó feltételek kiválasztása pedig még inkább az. Habár a láncolat első eseményét gyakran „kezd(eményez)ő eseménynek" nevezik, ennek kiválasztása önkényes, és mindig hozzá lehet adni korábbi eseményeket és feltételeket. A visszafelé haladó eseménylánc-elemzésekben – például az eseményfa elkészítése során – a megállási pont kiválasztásának szubjektivitása azt jelenti, hogy a baleset „fő okának" kijelölése (is), az utólagos elemzéshez alkalmazott megállási szabály tekintetében tisztán pragmatikus kérdés – azaz nincs jól meghatározott „kezdete" a balesetek okozati láncának. Ennek feltételezhető oka, hogy a balesetek kivizsgálásának a korábbi időszakban többnyire két alapvető célja volt: az egyik a balesetért való felelősség megállapítása, a másik a baleset okának megértése annak érdekében, hogy a jövőbeni balesetek megelőzhetők legyenek. Ha a cél a hibáztatás, akkor a visszafelé haladó eseménylánc visszafejtési folyamata gyakran megáll annál a pontál,

[26] System-Theory Accident Model and Processes (STAMP).
[27] Massachusetts Institute of Technology (MIT).

ahol valakit vagy valamit felelőssé lehet tenni (hibáztatható) az esemény bekövetkezéséért. A hasonló veszteségek megelőzése szempontjából az ilyen elemzés túl felületes magyarázatot adhat arra, hogy miért is történt a baleset. A közelmúltban bekövetkezett – valamilyen módon szoftverrel kapcsolatos – repülőgép-balesetek elemzése során a legtöbb vizsgálat – többnyire – megállt a végrehajtó személy hibáztatásánál, és soha nem tért ki a baleset okának, gyökerének megállapítására – például arra, hogy az üzemeltetők miért követték el a hibákat, és hogyan lehet megelőzni ezeket a jövőben, vagy hogy miért hibás a szoftverrel kapcsolatos követelménytámasztási előírás, vagy a szoftver minőségi problémáit miért nem fedezték fel és javították ki, mielőtt alkalmazásba vették volna [9, p. 241].

A STAMP alaphipotézise, hogy a balesetek akkor következnek be, amikor a külső zavarokat, az alkatrészek meghibásodását, vagy a rendszerelemek közötti diszfunkcionális kölcsönhatásokat a szabályozó rendszer nem kezeli megfelelően, azaz a rendszer fejlesztésére, tervezésére és üzemeltetésére vonatkozó, biztonsággal kapcsolatos korlátozások nem megfelelő ellenőrzése vagy érvényesítése miatt történnek [10, p. 12].

A STAMP ugyanakkor nem elemzési módszer, hanem a balesetek bekövetkezésének módjával összefüggésben kialakított modell, illetve feltevések összessége. A STAMP-re épülő eljárások alternatívát biztosítanak a hagyományos biztonsági elemzési technikák alapjául szolgáló hibaeseménylánc-elemzéseknek (például az LCFEM[28] mint a hibafaelemzés, az eseményfa-elemzés) vagy a Reason-féle „svájcisajt-szeleteknek". Ahogyan a hagyományos hibaeseménylánc-modellek esetében az elemzési módszerek a balesetek bekövetkezésének okaira vonatkozó feltételezésekre, feltevésekre épülnek, úgy a STAMP-et alapul véve új elemzési módszerek is felépíthetők. Fontos kiemelni, hogy mivel egyes hibaeseménylánc-modell lehet a STAMP eljárásrendjének egy részhalmaza, a STAMP-re épülő eszközök tartalmazhatják a régebbi biztonsági elemzési technikákból származó összes eredményt [10, p. 12].

Leveson hangsúlyozta, hogy a biztonságirányítási rendszereknek folyamatosan ellenőrizniük kell a feladatokat, és korlátozásokat kell bevezetniük a rendszer biztonságának szavatolása érdekében. A STAMP-re épülő balesetek kivizsgálásának eljárásrendje arra összpontosít, hogy a meglévő szabályozások, ellenőrzések miért nem képesek felismerni vagy megelőzni a balesethez vezető változásokat. A STAMP alapján a többszörösen összetett rendszerek vonatkozásában kidolgozták a hibák osztályozásának módszerét, amely segít az eseményhez hozzájáruló tényezők azonosításában. Emellett a STAMP felhasználása kibővíti a balesetmegelőzési akadályok és védelmi vonalak megközelítését, erősíti a proaktív gondolkodást, valamint a kiemelt biztonsági teljesítménymutatók kiválasztására is képes [13, p. 16].

A FRAM-mel ellentétben Leveson nem egy modellalkotási módszert készített, hanem a STAMP-re épülve két külön eljárásrendet dokumentált, az egyik a kockázatok azonosítására és elemzésére szolgáló rendszerelméleti folyamatelemzés[29] (STPA), a másik a bekövetkezett események szakmai vizsgálatára alkalmazható, a rendszerelméleten alapuló okelemzés[30] (CAST). A következő fejezet alapvetően a kockázatelemzési szempontból készített eljárásrendet mutatja be.

[28] Linear Chain of Fault Event Model (LCFEM).
[29] System-Theory Process Analysis (STPA).
[30] Causal Analysis based on System-Theory (CAST).

6. Az STPA-módszer ismertetése

Az STPA egy relatív új, proaktív veszély- és kockázatelemzési módszer, amely akár már a fejlesztés során elemzi a feltételezett balesetek lehetséges okait, hogy a veszélyek kiküszöbölhetők vagy ellenőrizhetők legyenek [10].

Az STPA néhány előnye a hagyományos veszélyforrás-, illetve kockázatelemzési technikákkal szemben a következő:

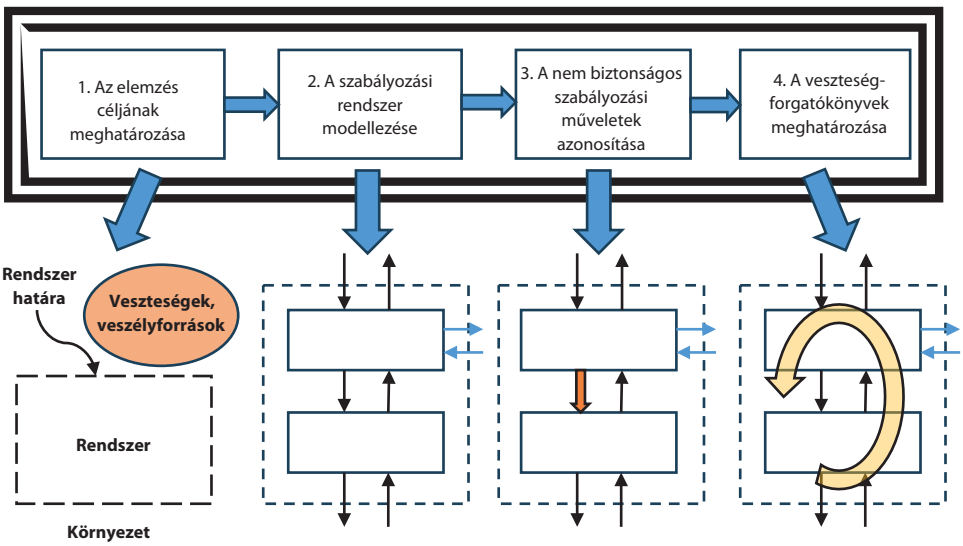
1. A STAMP alkalmazásával magas integráltsági fokú, összetett rendszerek kockázatai is elemezhetők. A korábban csak az üzemeltetés során felszínre kerülő kockázatok a fejlesztési folyamat korai szakaszában azonosíthatóvá és kiküszöbölhetővé, illetve az esetleges negatív hatásaik mérsékelhetővé válnak.
2. A hagyományos veszély-, illetve kockázatelemzési módszerekkel ellentétben az STPA-t a biztonsági követelmények és korlátozások azonosításának érdekében már a korai tervezési fázisban, a koncepcióelemzés során alkalmazni lehet. Ezek eredményét ezt követően fel lehet használni a biztonsági (és a védelmi) rendszerarchitektúra kialakításába és tervezésébe történő beépítéshez, kiküszöbölve a költséges utómunkálatokat, amikor a tervezés hibáit a fejlesztés vagy az üzemeltetés során későn azonosítják. A tervezés finomításával és a részletesebb tervezési döntések meghozatalával párhuzamosan, illetve annak következményeként az STPA-elemzést is finomítják, hogy segítse az egyre részletesebb döntések meghozatalát. Az STPA alkalmazásával végrehajtott tervezés során a teljes folyamat nyomonkövethetősége könnyen fenntartható a követelményektől az összes elkészült rendszer-alkotóelemig, ami javítja a rendszer karbantarthatóságát és fejlődését.
3. Az STPA a magas integráltsági fokú rendszerek minden elemét, a szoftvert és az emberi kezelőszemélyzetet is bevonja az elemzésbe, ezáltal szavatolja, hogy a veszély- és kockázatelemzés a veszteségek minden lehetséges okozó tényezőjére kiterjedjen.
4. Az STPA a rendszerfunkciók leírásáról dokumentációt biztosít, amely gyakran hiányzik vagy nehezen hozzáférhető a nagy, összetett rendszerekben.
5. Az STPA könnyen integrálható a rendszertervezési folyamatba és a modellalapú rendszertervezésbe [10, p. 4].

Számos értékelés és összehasonlítás készült az STPA-ról és a hagyományos[31] kockázatelemzési módszerekről, amelyek eredményeként kimutatható volt, hogy az STPA megtalálta az összes olyan ok-okozati összefüggést, amelyet a hagyományos elemzések is feltártak, emellett számos további, gyakran szoftveres alkalmazással kapcsolatos kockázatot/veszélyforrást, illetve veszteség-forgatókönyvet is azonosított, amelyeket a hagyományos módszerek nem fedtek fel. Néhány esetben, amikor olyan baleset történt, amelynek okairól az elemzőknek nem volt információjuk, csak az STPA találta meg a baleset tényleges okát. Ezen túlmenően a többszörösen összetett, bonyolult rendszereknél az STPA idő- és forrásigény szempontjából sokkal kevésbé bizonyult költségesnek, mint a hagyományos módszerek [10, p. 4].

[31] Például hibafa, eseményfa, HAZOP stb.

6.1. Az STPA alapeljárása

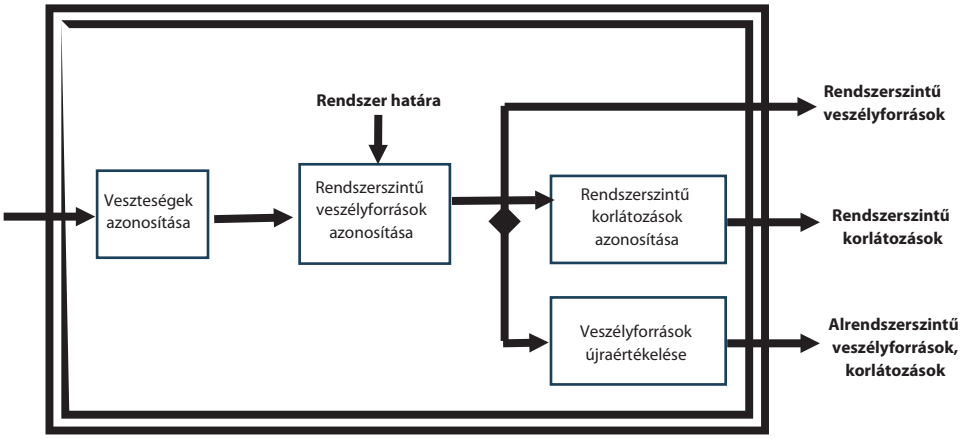
Az STPA-kézikönyv alapján az eljárás négy alapvető lépést tartalmaz, amelyet a 6. ábra szemléltet.



6. ábra
Az STPA-elemzés folyamatábrája (a szerző [10, p. 14] alapján)

6.2. Az elemzés céljának meghatározása

Itt meg kell határozni a lehetséges károkat, *veszteségeket,* a *rendszerszintű veszélyforrásokat,* a *rendszer működési korlátozásait,* emellett a kapott eredmények hatására adott esetben a veszélyforrásokat felül kell vizsgálni, ezáltal *alacsonyabb/alrendszer szintű veszélyforrások* és *korlátozások* kerülhetnek a felszínre (7. ábra).



7. ábra
Az elemzés céljának meghatározása az STPA első lépéseként (a szerző [10, p. 14] alapján)

A *veszteségek meghatározásakor* az alapelv az, hogy az érintettek számára (szervezet, személy) elfogadhatatlan veszteség tartozhat ide.[32] Ezeket sorra kell venni, és meg kell határozni, hogy a kockázatelemzés mely veszteségek elkerülése érdekében készül.

A *rendszerszintű veszélyforrások* leírásánál elsőre meg kell határozni a vizsgált rendszert, annak határait[33] és környezetét. Ha a rendszer meghatározása sikerült, akkor meg kell keresni a *rendszerszintű veszélyforrásokat,*[34] amelyek olyan rendszerállapotok vagy feltételek lehetnek (ide nem értve például az alkatrészszintű okokat vagy környezeti állapotokat), amelyek a legrosszabb környezeti feltételek esetén veszteséghez vezetnek, azaz veszélyforrásokon olyan állapotokat vagy körülményeket értünk, amelyeket meg kívánunk előzni.

A *rendszer működési korlátozásai* olyan rendszerfeltételeket vagy viselkedési formákat jelentenek, amelyeknek meg kell hogy feleljen a rendszer a veszélyek (és végső soron a veszteségek) megelőzése érdekében. A rendszerszintű veszélyforrások azonosítása után egyszerű behatárolni a rendszer működési korlátozásait, egyszerűen meg kell fordítani a veszélyforrások feltételeit.[35]

[32] Például az emberi élet elvesztése vagy sérülése, vagyoni kár, környezetszennyezés, küldetés ellehetetlenülése, hírnévvesztés, érzékeny információk elvesztése vagy kiszivárgása stb. [10, p. 16].

[33] A mérnöki munka szempontjából a rendszerhatár meghatározásának leghasznosabb módja, ha a rendszer vizsgálata azon részekre terjed csak ki, amelyekre a rendszer tervezőinek van ráhatásuk, kontrollt tudnak gyakorolni felette. Könnyen belátható, hogy a rendszer a környezetben felépített és a rendszer határai által elkülönülő, egymással együttműködő alrendszerekből áll, amelyek bemenete a környezetből eredeztethető, a kimenete pedig a környezet felé továbbítja a rendszer produktumát [10, p. 17].

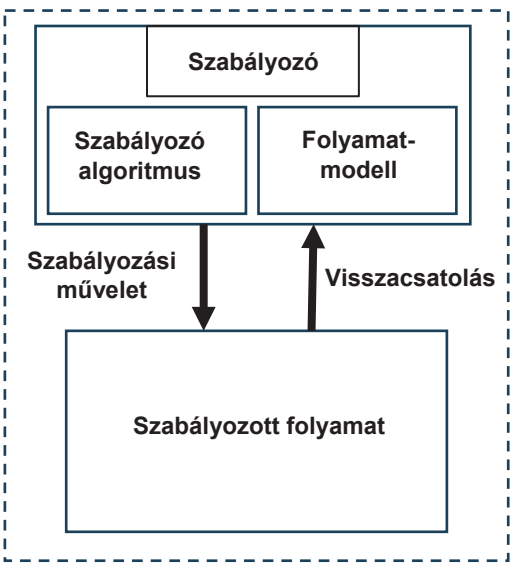
[34] Különbséget kell tenni a veszélyforrások és a veszteségek között: a veszteségek a környezet olyan aspektusait érinthetik, amelyek felett a rendszer tervezője vagy üzemeltetője csak részben, vagy egyáltalán nem rendelkezik ellenőrzéssel. A biztonságtechnika célja a veszélyek hatásainak kiküszöbölése vagy mérséklése az elemzett rendszerben, ezért bizonyos szintű ellenőrzésre van szükség [10, p. 17].

[35] Például ha légi jármű üzemeltetése során a rendszerszintű veszélyforrás a légi járművek, tereptárgyak közötti minimális elkülönítés megsértése, akkor a rendszer működési korlátja az, hogy a „rendszernek" be kell tartania a minimális elkülönítésre vonatkozó előírásokat [10, p. 20].

A *veszélyforrások felülvizsgálata,* az *alacsonyabb szintű veszélyforrások* és *korlátozások* meghatározása ugyan nem szükséges az STPA alkalmazásához, de ettől függetlenül hasznos kiegészítői lehetnek az összetett rendszerek elemzésének, mivel irányt mutathatnak a későbbi lépések, mint például a szabályozási rendszer modellezése esetén. Ehhez azonosítani kell azon alapvető folyamatokat vagy tevékenységeket a részrendszerben, amelyeket a rendszerszintű veszélyforrások, illetve kockázatok megelőzése érdekében ellenőrizni kell [10, pp. 14–22].

6.3. A szabályozási rendszer modellezése

A hierarchikus szabályozási rendszer egy olyan rendszermodell, amely irányítási folyamatokból és visszacsatolásokból (vezérlőhurkokból) áll, és amely a teljes rendszer működésére és viselkedésére nézve strukturális szabályozásokat érvényesít. Általában *a szabályozó* (vezető) döntéseket hoz a célok elérése érdekében, és *szabályozási műveleteket* hajt végre bizonyos folyamatok irányítása/vezérlése és a szabályozott folyamat viselkedésére vonatkozó korlátozások érvényesítése érdekében.



8. ábra
Általános szabályozási rendszer (hurok) (a szerző [10, p. 23] alapján)

A 8. ábrán látható, hogy a *szabályozott folyamat* egy fizikai folyamat vagy egy másik szabályozó irányítása lehet. A *szabályozó algoritmus* a vezető döntéshozatali folyamatát jeleníti meg – ez határozza meg a végrehajtandó szabályozási műveleteket.

A szabályozó önmagában is rendelkezik *folyamatmodellekkel,* amelyek belső döntéshozatali eljárásrendjét jelenítik meg. Ezen folyamatmodellek emellett tartalmazhatják a szabályozó elgondolását, képét az általa irányított folyamatról, a rendszer vagy a környezet egyéb releváns aspektusairól. A szabályozó a *szabályozási műveletek* kiadásával befolyásolja a szabályozott

folyamatot. A szabályozó a folyamatmodelleket részben az irányított folyamat megfigyeléséhez használt visszajelzések *(visszacsatolás)* alapján felülvizsgálhatja, módosíthatja.

Problémák a szabályozási rendszer bármely pontján keletkezhetnek.[36] A valóságban megjelenő hierarchizált rendszerekben megtalálhatók a fenti elemek, azaz a szabályozó, a szabályozási műveletek, a visszacsatolás, az irányított folyamat, illetve ezt kiegészítik még egyéb, a rendszer elemeitől érkező *bemeneti* vagy azok felé távozó *kimeneti jelek, folyamatok*.

A modellkészítés lépéseinek megkezdéséhez minimálisan legalább egy szabályozó, egy szabályozási művelet és egy szabályozott folyamat szükséges. Az elemzés kezdődhet egy hiányos struktúrával is, ilyenkor az STPA segít azonosítani az esetlegesen hiányzó visszajelzéseket, ellenőrzéseket és egyéb hiányosságokat, így a szabályozási struktúra a fejlesztéssel párhuzamosan finomítható. Adott rendszer szabályozói rendszerének modellezése során a 8. ábra szerinti alapmodell kibontását kell végrehajtani, figyelemmel arra, hogy minden rendszer más és más tulajdonságokkal, valamint alrendszerekkel rendelkezik. Az STPA végrehajtása során ezt olyan körfolyamatként kell kezelni, amely minden egyes ciklusban új felelősségi körök felbukkanása során további részleteket ad a modellhez. Általánosságban elmondható azonban, hogy az STPA elvégzése könnyebb és hatékonyabb lesz, ha a releváns információk szándékosan nem hiányoznak a vezetési struktúrából [10, pp. 22–34].

6.4. A nem biztonságos szabályozási műveletek azonosítása

A nem biztonságos szabályozási művelet[37] (UCA) definíció szerint olyan tevékenység, amely adott körülmények között (a legrosszabb esetben, a legrosszabb környezeti körülmények fennállása esetén) annak végrehajtása vagy a végrehajtás elmaradása esetén a rendszerben veszélyforrás megjelenéséhez vagy veszélyhelyzet kialakulásához vezet. Emellett UCA-nak tekinthetők azon műveletek is, amelyek noha *potenciálisan biztonságosak,* de egy folyamat vezérlése során *túl korán, túl későn vagy rossz sorrendben* hajtják őket végre, vagy adott esetben *túl sokáig tartanak, vagy túl korán* befejeződnek.

Minden UCA esetében meg kell határozni, hogy az adott szabályozási művelet milyen feltételek mellett (milyen kontextusban) nem biztonságos. Ezután ezeket az eseteket ki lehet zárni a rendszertervezésből, vagy meg lehet találni az esetleges kármérséklés módját. Egy UCA esetében bármilyen releváns kontextust meg lehet hivatkozni, beleértve a környezeti feltételeket, a szabályozott folyamat állapotát, a szabályozó állapotát, a szabályozó korábbi műveleteit (például ismétlődő műveletek), más szabályozók állapotát és korábbi műveleteit, egyidejű vagy ellentétes műveleteket, a szabályozási művelet paramétereit vagy tulajdonságait, vagy bármely más releváns feltételt.

Az UCA-k meghatározásakor fontos kiemelni, hogy az STPA-t ideális esetben még azelőtt célszerű alkalmazni, hogy bizonyos folyamatvédő automatizmusok ismertek lennének és beépülnének a tervezés alatt álló rendszerekbe. Az STPA egyik feladata ugyanis az, hogy

[36] Ha a szabályozott folyamat nem konzisztens a valósággal, az olyan szabályozási műveletekhez vezethet, amelyek veszélybe sodorhatják a rendszer működését. Ha például a visszacsatoló szenzor nem megfelelően működik egy rendszerben, az nem biztonságos rendszerműködéshez vezethet [10, p. 23].

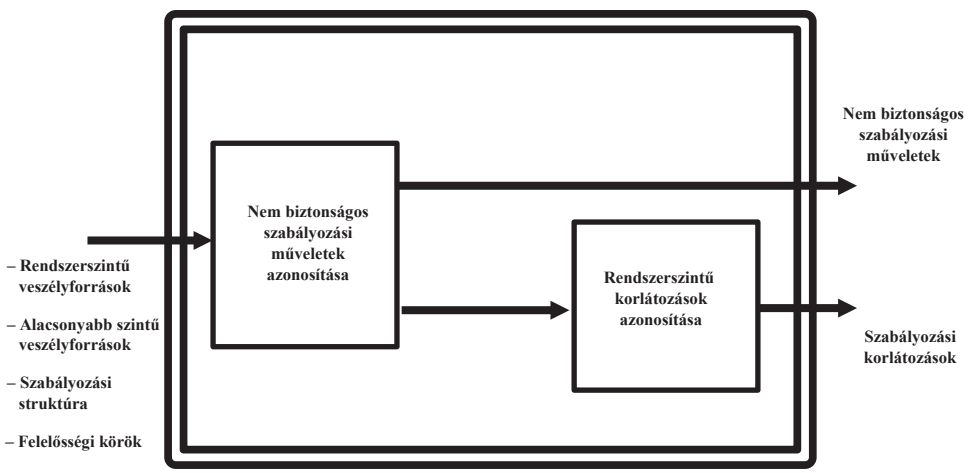
[37] Unsafe Control Action (UCA).

azonosítsa azokat az UCA-kat, amelyeket meg kell előzni, illetve ezt követően az UCA-kat felhasználva meghozza a funkcionális követelmények levezetéséhez szükséges és az UCA-k megelőzésére vagy mérséklésére irányuló tervezési döntéseket. A potenciális nem biztonságos rendszerviselkedés azonosítása után létre lehet hozni a konkrét tervezési jellemzőket, és hozzá lehet adni a folyamatvédő automatizmusokat, biztosító rendszereket (ha a terv még nem létezik), vagy meg lehet határozni a meglévő tervezési döntések és biztosító rendszerek megfelelőségét (ha a terv már létezik).

Minden UCA a rendszerszintű hatásain és eredményein keresztül a veszélyforrásokra vagy alacsonyabb szintű veszélyforrásokra mutat rá. Sok rendszer esetében az UCA és a veszélyforrások közötti kapcsolat egyértelmű és nyilvánvaló, néhány esetben azonban összetettebb, vagy éppen nem egyértelmű.

Az UCA-k vizsgálatába be kell vonni az ember által elkövetett vagy elkövethető nem biztonságos tevékenységeket (hibákat) is. Az STPA elmélete szerint az emberi tevékenységet ugyanúgy a rendszer részének kell tekinteni, amely így könnyen integrálhatóvá válik az elemzés elkészítésének folyamatában.

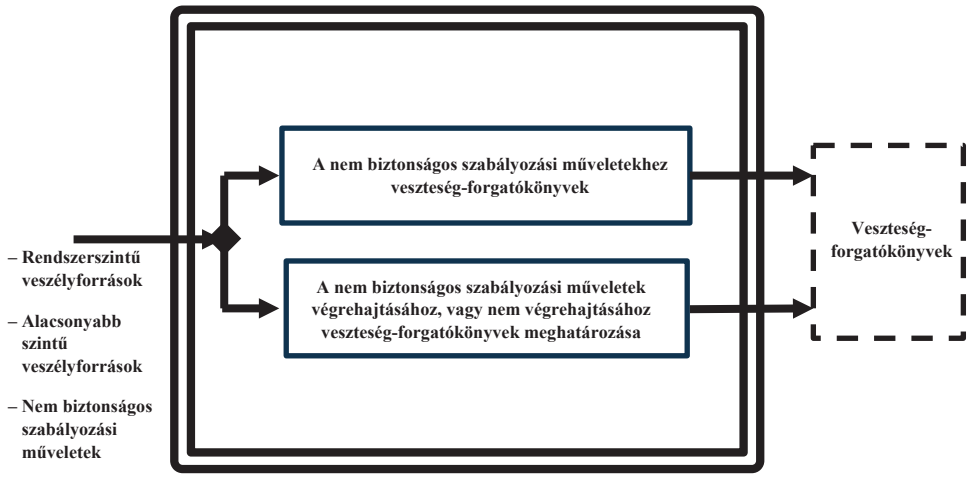
Az UCA-k összesítése végén meg kell határozni a *szabályozói korlátozásokat,* amelyek azon szabályozói viselkedések összességét jelentik, amelyeknek a szabályozást végző folyamat meg kell hogy feleljen az UCA-k megelőzése érdekében (9. ábra) [10, pp. 34–42].



9. ábra
A szabályozási műveletek vizsgálatának áttekintése (a szerző [10, p. 42] alapján)

6.5. A veszteség-forgatókönyvek meghatározása

A veszteség-forgatókönyv leírja azokat az ok-okozati tényezőket, amelyek UCA-k és veszélyhelyzetek kialakulásához vezethetnek.



10. ábra
A veszteség-forgatókönyvek meghatározásának folyamata (a szerző [10, p. 52] alapján)

A 10. ábrán látható, hogy az STPA záró alaplépésénél a rendszerszintű veszélyforrásokból, az esetlegesen feltárt alrendszer szintű veszélyforrásokból, a szabályozási struktúra tulajdonságaiból, illetve az UCA-k hatásaiból meg kell határozni azokat az ok-okozati összefüggéseket, amelyek az UCA-k kialakulásához, illetve a szabályozási műveletek nem megfelelő végrehajtásához, vagy éppen végre nem hajtásához vezettek [10, pp. 42–53]. Ezen folyamatok elemzéséből levezethetők azon biztonsági követelmények vagy kockázatcsökkentő intézkedések, eljárások, amelyek az összetett rendszer biztonságosabb üzemeltetését hivatottak biztosítani.

6.6. Az STPA eredménye és visszakövethetősége

Az STPA feltárja egy vizsgált rendszer UCA-k alkalmazásával meglévő veszélyforgatókönyveit, a szabályozási korlátozásokat és ezek együttes hatását az UCA-k kialakulására. Emellett megmutatja a felelősségi körök kiosztásának hatását a rendszerszintű korlátozásokra. Összefoglalja a fentiek összesített befolyását a rendszerszintű veszélyforrásokra, amelyekre szintén hatnak az UCA-k alkalmazása nélküli veszteség-forgatókönyvek. Végül megmutatja a rendszer lehetséges veszteségeit.

Az STPA kimenetén megjelenő eredmények felhasználhatók, többek között egy rendszer-architektúra szabályozására, megfelelő rendszerkövetelmények létrehozására, tervezési ajánlás megfogalmazására, a szükséges kockázatcsökkentő eljárások és védelmi tevékenységek azonosítására. Emellett segítenek a megfelelő tesztelési pontok meghatározásában és a teszttervek elkészítésében, az új tervezési döntések meghozatalában.[38] Az eredmények felhasználhatók továbbá a meglévő tervezési döntések értékeléséhez, valamint a hiányosságok

[38] Amennyiben a fejlesztés során STPA alkalmazása mellett döntöttek a tervezők.

és a szükséges változtatások azonosításához.[39] Nem utolsósorban az eredmények elősegítik a kockázatkezelés során alkalmazott kiemelt biztonsági mutatók meghatározását és a hatékonyabb biztonságirányítási rendszerek kialakítását [10, p. 52].

6.7. A STAMP és az STPA további alkalmazása a biztonsági mutatók meghatározásában a kockázatok kezelése során

Minden biztonságos működés megvalósítását célzó rendszernek, így a repülésbiztonság-irányítási rendszernek is egyik alapeleme a fellépő kockázatok kezelése. A kockázatok kezelési rendszere (kockázatmenedzsment) nehezen elképzelhető olyan indikátorok alkalmazása nélkül, amelyek az adott rendszer működéséről összegyűjtött információk közül kiemelten fontos tulajdonságokkal bírnak, ezáltal képesek jelezni az adott rendszer biztonságos működésében bekövetkezett negatív változásokat.

Ezek a mutatók a légi közlekedésben többnyire a kockázatok valószínűsége szerint vannak meghatározva.[40] Ugyanakkor a STAMP modellen alapuló STPA-eljáráshoz kötötten – Leveson elmélete szerint – a hasznosnak tekinthető *kiemelt* (biztonsági) *mutatókat*[41] a mérnöki gyakorlati *tapasztalatok* és a vizsgált rendszerek sebezhetőségének alapjául szolgáló, kritikusnak tekintett *felvetések* mentén lehet azonosítani, nem pedig a káresemények valószínűsége alapján [11, p. 20].

A biztonságot érintő kritikusnak tekintett *felvetéseket* a STAMP-modell segítségével az alábbiak mentén szükséges csoportosítani:

1. a rendszer veszélyeiről és a veszélyekhez vezető okokról kialakított felvetés;[42]
2. azok a felvetések, amelyek a veszélyek csökkentésére vagy kezelésére alkalmazott szabályozási műveletek hatékonyságára vonatkoznak;
3. a rendszer üzemeltetésének módjára és a környezetre (kontextusra) vonatkozó felvetések, amelyben a rendszer működni fog;[43]
4. a fejlesztési környezetre és folyamatokra vonatkozó felvetések;
5. az üzemeltetés során a szervezeti és társadalmi biztonságszabályozási struktúráról kialakított felvetések.[44]

[39] Amennyiben a tervezés befejezése után továbbra is az STPA-eljárást alkalmazzák a tervezők.

[40] Példaként a Boeing gyár a B-787-es repülőgépek esetében azt feltételezte a lítiumion-akkumulátorok meghibásodása kockázatának becslésekor, hogy a valószínűség 1 eset a 10 000 000 repült órára lebontva, de a tényleges esemény kétszer fordult elő az első 52 000 repült óra alatt [11, p. 19].

[41] Leveson a kiemelt mutatókon olyan figyelmeztető jeleket ért, amelyek egy biztonságkritikus folyamat felügyelete során használhatók annak észlelésére, ha egy biztonsággal kapcsolatos feltételezés megszűnik vagy veszélyesen gyengévé válik, és a baleset megelőzése érdekében intézkedésre van szükség [11, p. 20].

[42] Új veszélyek merülhetnek fel, vagy a meglévő veszélyek ok-okozati elemzésének alapjául szolgáló feltételezések, felvetések változhatnak [11, pp. 24–25].

[43] Feltételezzük, hogy egy rendszer vezérlése a tervezők által meghatározott módon fog történni. Ugyanakkor az emberi viselkedésre vonatkozó felvetések különösen sérülékenyek, mivel az emberek idővel hajlamosak alkalmazkodni a működési környezethez vagy a gyakorlatban alkalmazott eljárásrendektől való „praktikus" eltéréshez [11, p. 24–25].

[44] Azaz hogy minden a terveknek megfelelően működik, a tervezés megfelelő volt a rendszer biztonsági követelményeinek érvényesítéséhez, illetve a rendszerirányítók teljesítik biztonsági feladataikat, és a terveknek megfelelően működnek. Ilyen feltételezések közé tartoznak a biztonsági kultúra állapotára vonatkozó feltételezések, például hogy a szervezeti biztonsági irányelveket követi-e, vagy sem [11, p. 25].

A kockázatértékelésben a sebezhetőségre vagy a kockázat súlyosságára vonatkozó felvetések.[45] [11, pp. 24–25].

A megfelelő és hatékony kiemelt mutatók – legalábbis részben – az STPA segítségével azonosíthatók, oly módon, hogy a fentebb említett hierarchikus szabályozási struktúra modelljét és a szervezetbe épített ellenőrzéseket felhasználva azonosítjuk azokat a felvetéseket, amelyeken a FRAM-módszer esetében is említett „felbukkanó" (biztonsági) rendszertulajdonságokra vonatkozó korlátozások alapulnak, és meghatározzuk, hogyan lehet észlelni a rendszer céljainak elérésére tervezett ellenőrzések hatékonyságának gyengülését [10, p. 101].

Az STPA négy alaplépésén keresztül a biztonságkritikus felvetések meghatározhatók a kapcsolódó biztonsági célok, a működéshez szükséges szabályozási rendszerrel kapcsolatos összefüggések vizsgálatával, és feltárhatók a felmerülő UCA-kkal való kapcsolódási pontok is.

A biztonságkritikus felvetések egyik alapvető csoportja szerint egy megfelelően megtervezett és üzemeltetett rendszerben nem fordulnak elő veszélyforrások és kockázatok. Ugyanakkor bármely veszélyforrás megjelenése vagy esemény bekövetkezése (még akkor is, ha nem vezet balesethez) a biztonsági folyamatok teljes felülvizsgálatát kell hogy kiváltsa. A veszélyforrások azonosítása kiindulópontként szolgálhat, amelyből az STPA használatával a veszélyforrásokhoz vezető (veszteség-)forgatókönyvek azonosítására további ellenőrzések vezethetők le [10, p. 109]. A kiemelt indikátorok ezen veszélyforrások előrejelzésére szolgálnak.

7. Összegzés

A technológiai fejlődés folyamatos gyorsulásának eredményeként a légi járművek fejlesztése egyre komplexebb rendszereket hoz létre, amelyek már nemcsak mechanikai tulajdonságaik szerint lesznek egyre bonyolultabbak, hanem az alkalmazott és azokat működtető szoftverek integráltsági fokát tekintve is mind nagyobb kihívásokat jelentenek. A lineáris kockázatelemzési eljárások napjainkra elérték a működési korlátjaikat, azaz ezen rendszerek részletes analízise csak bizonyos mértékű egyszerűsítés mellett végezhető el.

A jelen cikkben bemutatott – kifejezetten ilyen többszörösen összetett, integrált rendszerek vizsgálatára kialakított – modellek lehetőséget biztosítanak ezen bonyolult rendszerek tervezésének támogatására, a működésük megértésére, a felmerülő veszélyforrások és kockázatok azonosítására.

A FRAM- és a STAMP/STPA-módszerek ugyanazon problémára két különböző megközelítési módot képviselnek. Céljuk a bonyolult, többszörösen összetett, magas integráltsági fokú rendszerek olyan modellezése, amely alkalmas a működésükben rejlő veszélyforrások, kockázatok és a lehetséges veszteségek azonosítására, elemzésére.

Ugyanakkor kár lenne tagadni, hogy akár a FRAM-, akár a STAMP-módszerre épülő STPA-eljárás megértése, alkalmazása nem egyszerű feladat. A FRAM esetében online esettanulmányok is elérhetők a módszer alapjainak jobb elsajátítása érdekében, illetve külön számítógéppel támogatott vizualizációs alkalmazás kifejlesztésére is sor került az elmúlt időszakban. A fejlesztők honlapján FRAMily néven kisebb közösséget építenek a FRAM-felhasználók között, illetve rendszeres konferenciák népszerűsítik a módszert.

[45] Ezek idővel változhatnak, és így magának a kockázatkezelési és a kiemelt indikátorok rendszerének újratervezését teszik szükségessé [11, p. 25].

Mindkét eljáráshoz külön kézikönyvet adtak ki, amelyek példákkal illusztrálva igyekeznek „emészthetőbb" formába önteni az elemzési folyamatokat. A FRAM mellett a STAMP módszer is rendelkezik internetes támogatással STAMP Workshop néven, itt az MIT szerverén elérhető az eddig kiadott dokumentációk, képzési és alkalmazási segédletek.

Az eddigi ismeretek szerint a STAMP modell alkalmazása egyelőre kevéssé terjedt el a biztonsággal foglalkozó szakmai közösségben, és nem ismerik annyira széles körben, mint a lineáris vagy komplex lineáris eseménymodelleket, emiatt jelenleg vélhetően kisebb hatást gyakorol a balesetek modellezésére, illetve általában a biztonságirányítási rendszerekre. Ennek egyik oka lehet a modell komplexitása, a másik pedig az, hogy nem alkalmazza a széles körben használatos adatgyűjtési és adatelemzési eljárásokat, hiszen dedikáltan más célokat fogalmaztak meg a fejlesztők [13, pp. 16–17].

A University of Southern California, Viterby, Schools of Engineering, Aviation Safety and Security Program oktatójával – aki egyben az American Airlines repülésbiztonsági vezetője is[46] – 2024 szeptemberében folytatott informális megbeszélés során elhangzott, hogy az American Airlines légitársaságnál bizonyos balesetek, illetve működési kockázatok feltárásakor tapasztaltak alapján a STAMP egy kiváló rendszerelméleti eljárásrend, amelynek alkalmazása magas fokú hozzáértést és képzettséget feltételez, az elemzés elvégzése a vizsgált folyamat, rendszer bonyolultsági fokától függően meglehetősen időigényes feladat.

Ebből kifolyólag a STAMP elemzési folyamat előnye mindenképpen a komplex, integrált rendszerek elemzési lehetőségében áll, ugyanakkor a profitorientált világban – ahol a műveletek végrehajtási kényszere, az időhiány, a bekerülési költségek és a haszon közötti kötéltánc folyamatos nyomás alá helyezi a rendszerbiztonsággal foglalkozó szakembereket – az elemzési módszer viszonylagos bonyolultsága kihívásokat állít a módszer elterjedése elé.

Összességében a két bemutatott módszer, habár különböző megközelítés mentén, egy fontos paradigmaváltást készíthet elő a (légi közlekedési) balesetek, események modellezésében, valamint a kockázatelemzések elkészítésében.

Felhasznált irodalom

[1] D. Viner, *Accident Analysis and Risk Control,* Melbourne, Derek Viner Pty Ltd, 1991.

[2] E. Hollnagel, D. Slater, *A FRAM Handbook,* FRAMsynt 2022.

[3] E. Hollnagel, *An Application of the Functional Resonance Analysis Method (FRAM) to Risk Assessment of Organisational Change,* Stockholm, Swedish Radiation Safety Authority, 2013. Online: https://inis.iaea.org/collection/NCLCollectionStore/_Public/44/057/44057156.pdf

[4] E. Hollnagel, *Barriers and Accident Prevention,* London, Ashgate Publishing, 2004.

[5] E. Hollnagel, *FRAM Model Interpeter,* FRAMsynt 2021. Online: https://safetysynthesis.com/onewebmedia/FMI_Plus_V2-1.pdf

[6] E. Hollnagel, Ö. Goteman, "The Functional Resonance Accident Model," in *Cognitive Systems Engineering in Process Control,* Sendai, Tohoku University 2004. Online: https://skybrary.aero/sites/default/files/bookshelf/403.pdf

[46] John de Leeuw, Managing Director Safety and Efficiency, American Airlines.

[7] J. Rasmussen, „Human Error and the Problem of Causality in Analysis of Accidents." *Philosophical Transactions of the Royal Society, Biological Sciences,* 327. évf. 1241. sz. pp. 449–462. 1990. Online: https://doi.org/10.1098/rstb.1990.0088
[8] J. Larouzee, J.-C. Le Coze, „Good and Bad Reasons: The Swiss Cheese Model and Its Critics," *Safety Science,* 126. évf. 2020. Online: https://doi.org/10.1016/j.ssci.2020.104660
[9] N. Leveson, „A New Accident Model for Engineering Safer Systems," *Safety Science,* 42. évf. 4. sz. pp. 237–270. 2004. Online: https://doi.org/10.1016/S0925-7535(03)00047-X
[10] N. G. Leveson, J. P. Thomas, *STPA Handbook,* MIT Partnership for System Spproaches to Safety and Security (PSASS), Boston, Massachusetts Institute of Technology, 2018. Online: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf
[11] N. G. Leveson, „A Systems Approach to Risk Management Through Leading Safety Indicators," *Reliability Engineering and System Safety,* 136. évf. pp. 17–34. 2015. Online: https://doi.org/10.1016/j.ress.2014.10.008
[12] R. Patriarca et al., „Framing the FRAM: A Literature Review on the Functional Resonance Analysis Method," *Safety Science,* 129. évf. 2020. Online: https://doi.org/10.1016/j.ssci.2020.104827
[13] Y. Toft et al., *Model of Causation: Safety,* Tullamarine, Safety Institute of Australia Ltd. 2012.

The Evolution of Risk Analysis in Aviation Safety II

As many hazardous operations, aviation can only be carried out on the basis of acceptable and unacceptable risks, i.e. risks that must be managed. The purpose of writing this article is to continue the presentation, possible interrelationship and usefulness of risk analysis procedures that have emerged since the 1960s. It is intended to describe risk analysis and visualisation procedures that can be applied to the analysis of complex, multi-integrated systems in addition to linear risk analysis procedures. However, understanding and applying the models that emerged after the 2000s is as complex a task as the systems they are designed to analyse. This article aims, among other things, to help in understanding this complex vision. The research method chosen was based mainly on a review of the foreign literature.

Keywords: *risk assessment, risk management, linear event model, komplex non-linear event modell, FRAM, STAMP, STPA*

Beller Balázs
vezető kiemelt főtiszt
HM Állami Légügyi Főosztály
Repülésbiztonsági és Repülőtérfelügyeleti Osztály
balub77@gmail.com
orcid.org/0009-0009-6117-1026

Balázs Beller
Senior Executive Staff Officer
MoD State Aviation Department
Flight Safety and Airport Operations Supervisory Division
balub77@gmail.com
orcid.org/0009-0009-6117-1026