Óbudai Egyetem

Doktori (PhD) értekezés

Gépjárműrendszerek megbízhatóság- és termékbiztonság szempontú előzetes kockázat elemzése

Ványi Gábor

Témavezető: Pokorádi László C.Sc.

Biztonságtudományi Doktori Iskola

Budapest, 2019

Szigorlati Bizottság:

Elnök:

Prof. Dr. habil. Berek Lajos, egyetemi tanár

Tagok:

Dr. Kavas László, egyetemi docens

Dr. Lázár-Fülep Tímea, egyetemi adjunktus

Nyilvános védés bizottsága:

Elnök:

Prof. Dr. habil. Berek Lajos, egyetemi tanár

Titkár:

Dr. Szűcs Endre, egyetemi docens

Tagok:

Dr. Johanyák Zsolt Csaba, főiskolai tanár

Dr. Farkas Gabriella, egyetemi adjunktus

Dr. Czifra Árpád, egyetemi docens

Bírálók:

Prof. Dr. habil. Abonyi János, egyetemi tanár

Dr. Fülep Tímea, egyetemi adjunktus

Nyilvános védés időpontja

……..

NYILATKOZAT A MUNKA ÖNÁLLÓSÁGÁRÓL, IRODALMI FORRÁSOK MEGFELELŐ MÓDON TÖRTÉNT IDÉZÉSÉRŐL

Alulírott *Ványi Gábor* kijelentem, hogy a *Gépjárműrendszerek megbízhatóság- és termékbiztonság szempontú előzetes kockázat elemzése* című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

Budapest, 2019. 02. 28.

TARTALOMJEGYZÉK

ELŐSZÓ

Napjainkban közlekedő járművek természetes építő elemévé vált az asztali számítógépek teljesítményét elérő beágyazott rendszerek sokasága, amelyek észrevétlenül végzik az összehangolt, bonyolult számításokat, környezetükből jövő változásokat érzékelik és alkalmazkodnak azokhoz a jármű biztonságos működését biztosítva. A különféle funkciók különböző beszállítók termékeként kerül beépítésre a járműben, hiszen az egyes funkcionalitás fejlesztéséhez speciális ismeret szükséges. A járművet gyártó cégnek több beszállító egyéni fejlesztését kell összehangolnia, amelyet az iparági minőségirányítási rendszeren túlmenően saját szabványaival és iparági szabványok, előírások elvárásával egységesít és szabályoz. Az előírásokat a megrendelni kívánt termék működési elvárásával (követelményeivel) együtt adja át a beszállítóknak, akik igyekeznek a saját fejlesztési folyamatuk szerint úgy végezni feladatukat, hogy a termékük biztonságosan működni tudjon a többi beszállító termékével.

A gazdaságos üzemeltetés, a környezetvédelemi előírások szigorodása és a mesterséges intelligencia térhódítása a járművekkel szembeni elvárásainkat átformálják. A gyártók igyekeznek ezeknek az új igényeknek is megfelelni, ezért sokszor a kiforrott műszaki megoldásokat újabb és bonyolultabb funkciókkal bővítik. A beszállítóknak meg kell felelniük ezeknek az igényeknek számos esetben rövid idő alatt, ha a piacon kívánnak maradni és meg akarják őrizni kedvező pozíciójukat. Az új termékkel szemben támasztott előírások (követelmények) sokszor kiegészítésre szorulnak, mert a vevő nem ismeri mélységében a megrendelni kívánt eszközt, csupán a járműben betöltött elvárásait tudja megfogalmazni. Mint említettem, a bonyolultság egyre növekszik, így egy termék mögött számos al-beszállító állhat, így nem ritka, hogy a megbízott beszállító további cégektől átvett terméket integrálja össze és adja át a megrendelőnek.

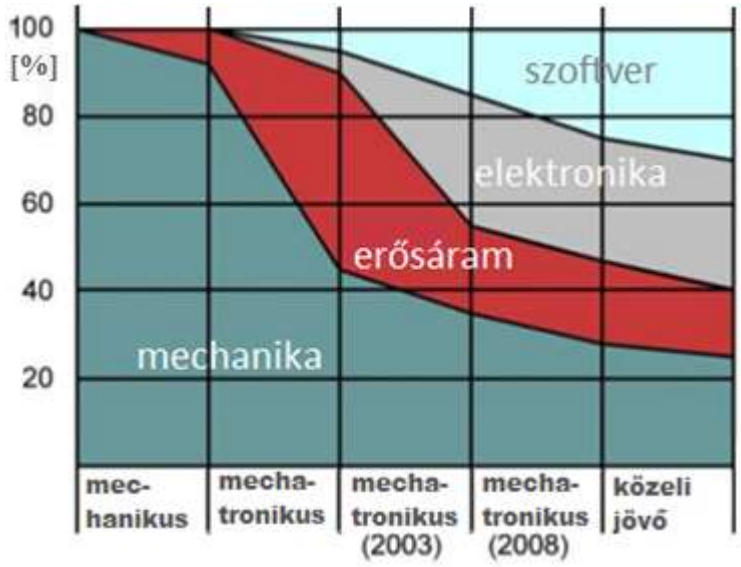
A termék minőségét ilyen kiterjedt munkavégzés mellett is biztosítani kell. A követelmények teljesítését tesztek futtatásával tudják bizonyítani, de ezzel még nem győződhettünk meg a biztonságos működésről. A műszaki megbízhatóságot és termék biztonságot felmérni és tervezni lehetséges, amelyre találhatóak előírások és ajánlások. A legáltalánosabban alkalmazott egyik módszer a hibamód és –hatáselemzés. A beszállítók a másik fél részrendszeréhez kapcsolódóan kell, hogy modellezzék saját rendszerüket, megvizsgálva az általuk fejlesztett funkciók meghibásodásából eredő kockázatokat.

A kockázatelemzést sokféle módon lehet elvégezni, nagyon eltérő eredményeket létrehozva. Maga a hibamód és –hatás elemzés 1949 óta ismert [51], de olyan megvalósítás, amely a mechanika mellett az elektronikus hardver- és szoftver modelleket is össze lehet kapcsolni csak az utóbbi évtizedekben fogalmazódott meg [41]. Megtapasztaltam, hogy a régóta alkalmazott módszert számtalan egyéni módon, sokszor kötelezettségnek eleget téve alkalmazzák – nem várva használható eredményt. Nagyon sok időt és kapacitást tud felemészteni és sokszor haszontalannak érzik az alkalmazását.

A kutatómunkám célja a szakmai elvárásoknak megfelelő, minőségi hibamód és –hatás kockázatelemzés készítésének elősegítése. A módszertan alapvető szabályait betartva gyakorlatban is alkalmazható eredményeket dolgoztam ki.

1 BEVEZETÉS

A munkám és kutatásom során azt tapasztaltam, hogy az autóipar, azon belül is a haszongépjárművek alapjában véve egy gépipari (mechanikai) fejlesztési módszerekre épülő háttérből alakult ki. Mára a járműrendszerek komplex rendszerré váltak, egyre több funkciót integrálnak a járművekbe. Ugyanakkor hatósági előírásoknak eleget téve csökkenteni kell az össztömegüket. A mechanikai vezérlő elemeket általában felváltja a szoftvert futtató elektronikus eszközök sora. A gyorsan változó, globalizált piac miatt egyre gyakrabban fordul elő egy fejlesztés folyamán, hogy kisebb-nagyobb változtatásokat kell bevezetni a terméken még a fejlesztési szakaszban, a sériagyártás indítása előtt vagy akár közben is. A szoftver tartalom növekedésével a jármű össztömege nem változik ugyan, de a funkciók száma és az összetettsége jelentősen nő. Több ezer előírást tartalmazó követelményhalmaz feldolgozása szükséges a megbízhatósági elemzések elvégzéséhez hatékonyan, amelyben kihívást jelent egy integrált hardver-, szoftver-, mechanikai rendszer átfogó modellezése az eltérő fejlesztési ütem, és fókuszpont tartalma miatt.



1.1. ábra Mechanika–elektronika–szoftver komponensek összetételének várhatóváltozása [10]

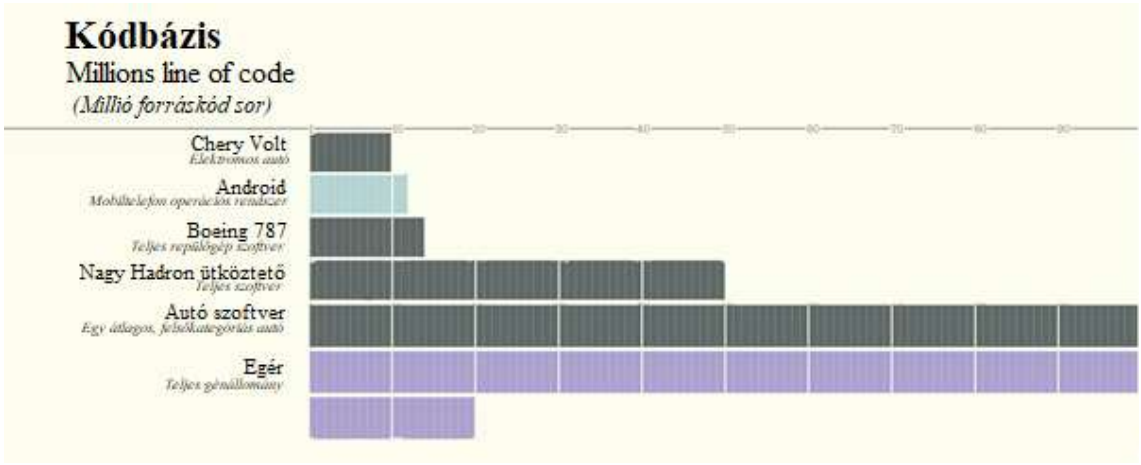
A járműipari szereplők felismerve az 1.1. ábrán látható trendet, illetve alapul véve a rendelkezésre álló közúti járművek meghibásodási statisztikákat, például a német autóklub (ADAC) személygépjármű [21] és haszongépjármű [92] alapján megállapítást nyert, hogy az elektronikus komponensek fejlesztését biztonságosabbá kell tenni. Egy iparági szabvány az ISO 26262 [33] [36], amelyet 2011-ben adtak ki először, a 3,5 tonnánál könnyebb

gépjármű személygépjárművekre vonatkozóan ugyan, de a haszongépjárművek fejlesztésében is figyelembe veszik az iparági szereplők. A szabvány a kockázat elemzését, osztályozását, rangsorolását írja elő, amely rangsorolás szerint teljesítendő munkacsomagokat a fejlesztési folyamatokban határozza meg. Az egyik alapvető elemzésként írja elő például a hibamód és -hatáselemzést a Failure Method and Effect Analysis (FMEA) módszer használatát elsődlegesen és magasabb kritikussági szinten kiegészíti az egyes elemi hibák kialakulásának mélyebb elemzését, így megértését a hibafa elemzést, Failure Tree Analysis (FTA)-t is [36].

Az értekezésem célja a gépjárműrendszerek funkcióinak műszaki kockázatelemzése a fejlesztési szakaszban, hogy minél korábbi fázisban használható eredményeket szolgáltasson a termék fejlesztéséhez. A rendelkezésre álló információk alapján pedig becsülhető legyen a rendszer megbízhatóságának színvonala, az elérhető követelmények és elsődleges tervek információból induló a vizsgálat, összefogva a különböző mérnöki területek eltérő igényeit. Dolgozatomban egyrészt az említett FMEA módszer alkalmazásához keresek megoldást egy egységesített rendszermodell felépítésével, az elektronikus hardver, szoftver és mechanikai elemek együttes modellbe foglalásával – csökkentve az elemzés elvégzéséhez szükséges kapacitást, növelve a korábbi elemzések eredményeinek újra felhasználhatóságát. Másrészt célom az FMEA elemzés eredményeit felhasználva finomítani a kritikus pontok megtalálását, rangsorolását. A kitűzött célok együttesével pedig a minőségbiztosítás támogatásának részeként, a kritikus pontok megismerésével a követelmények pontosítását és a termékbiztonsági elemzés eredmények prezentálhatóságát fejlesztettem. Ebből adódóan általánosítható eredmények várhatók az integrált biztonságkritikus rendszerek előzetes megbízhatósági elemzéseihez.

1.1 A gépjárműipari háttér

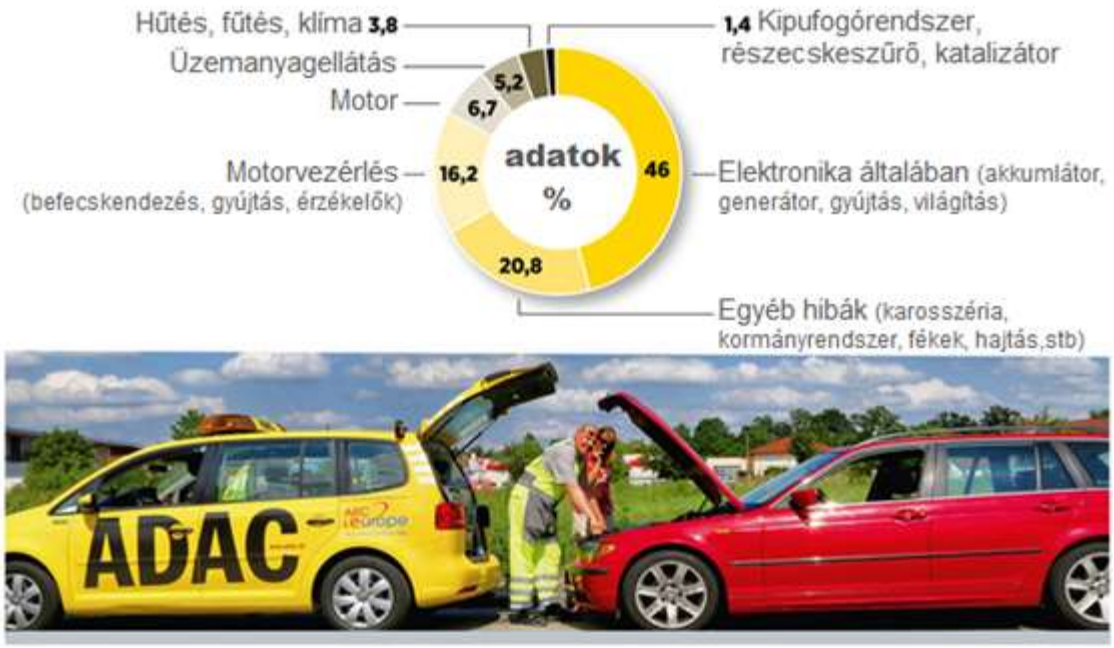
Egy átlagosnak tekinthető, felső kategóriás gépjármű rendszerében a szoftver nagysága az információtartalmat tekintve megközelíti egy egér teljes géninformáció tartalmát, amely 100 millió kódsorra tehető (1.2 ábra). Ha ezt kinyomtatnánk, akkor 1 800 000 oldalnyi szöveget tenne ki [19]. Az Audi A3-ban elsőként vált elérhetővé a mobiltelefon alapú negyedikgenerációs Long-Term Evolution (LTE) technológiát használó hotspot hozzáférés, amelyet a GM már tömeggyártásban is használ [58].



1.2. ábra Összehasonlítás az információtartalom tekintetében [19]

A távközlési technológiákat képviselő telekommunikációs terület és a gépjárműipar integrálódása, illetve a közösségi médiumok terjedéséből létrejövő új gépjárműhasználati szokások kialakulása terjed el. Az erőforrások gazdaságos kihasználásából és a környezetvédelemi előírások által megfogalmazódó új technológiai megoldások elérnek még a hajtáslánc technológiába is. Az elektronikus meghajtású járművek megjelenésével kezdetét vette a villamosítás, amit „electrification”-nak neveztek el [8]. Megfigyelhető az elterjedt szenzoros hálózatok (CAN, LIN, Flexray) jelentős száma a járművekben, amelyet újabb kommunikációs technológiával egészítenek ki a sebesség és a hálózatra csatlakozó eszközök számának növekedése és kommunikációs sebesség igénye miatt. Az újabb technológiára jellemző a már meglévő ismert műszaki megoldások, akárcsak az Ethernet technológia járműipari alkalmazásra késszé tétele [72]. Azonban fontos szemügyre venni a gépjárművekben tapasztalt meghibásodási statisztikákat is márkáktól függetlenül. Egy 2014-ben készült jelentésben a Német Autóklub (ADAC) felmérésében az elektronikus rendszerek meghibásodása az egyik leggyakoribb hiba ok (46%) a közúton a személygépjárművek körében [92], ahogy az 1.3 ábra mutatja.

Ezen a statisztikán pedig szükségszerű javítani, mert hiába kerülnek bevezetésre az egyre komfortosabb és korszerűbb elektronikai funkciók, ha az autó nem tud elszállítani megbízhatóan a kívánt úti célba és a meghibásodása esetleg emberi életet is kockáztat. Ezért a járműgyártók kidolgoztak egy funkcionális biztonságot bevezető szabványt személygépjárművekre, az ISO 26262-t [36]. Ez a szabvány lényegében a korábban közzétett IEC 61508 [73] biztonságkritikus rendszerek fejlesztésén alapul, de azokhoz képest elsősorban a hardver és szoftverfejlesztésre fókuszál [33].

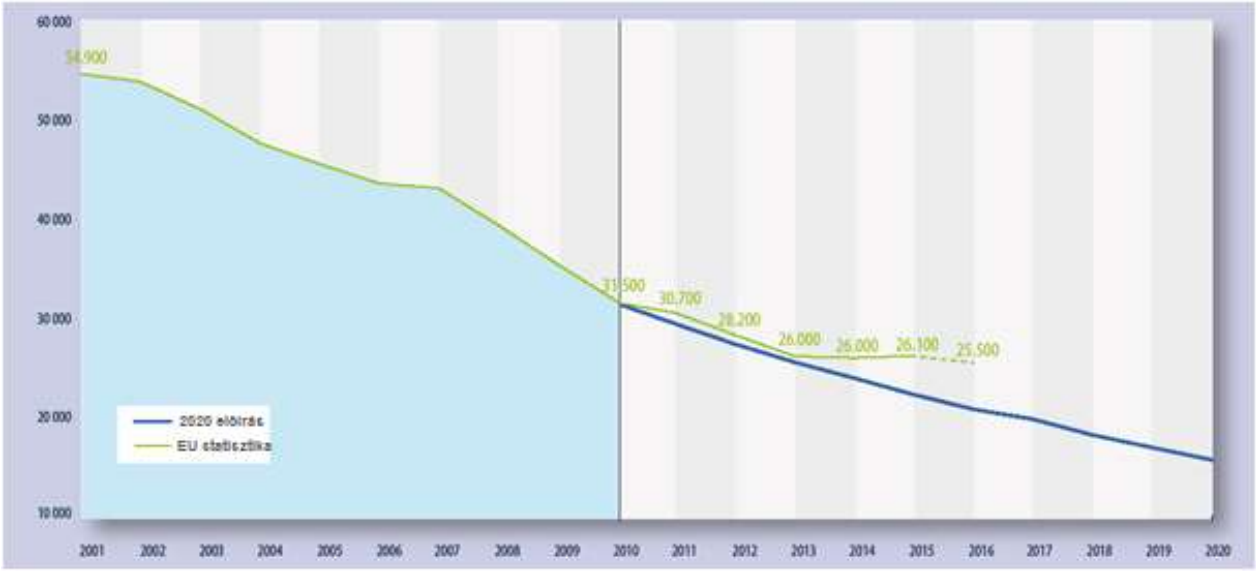


1.3. ábra A leggyakoribb hibák okai (2014) [20]

A mechanikai komponensek fejlesztésének biztonsági elemzése nem része az ISO szabványnak. A szabvány alkalmazásában nehézséget jelent a tudomány jelenlegi állásának (state of the art) bizonyítása, hiszen kellő számú rendeltetési körülmények között végzett terepi próbát, (field test) tapasztalatot kíván meg a terméken elvégezve, amely új járműrendszer korai fejlesztésénél nem áll még elegendő mennyiségben rendelkezésre. Továbbá maga a szabvány egyfajta követendő, legjobb tapasztalati alkalmazást (best practice) ad és nem deklarál minden esetben konkrét előírást az adott biztonsági szintnek megfelelően elvégzendő munkacsomagokra a fejlesztési- és tesztelési folyamatokban. Ilyen például, amikor egy fogalomra utal egy tudományos cikkből kiemelve. Bevezeti a társadalmilag elfogadott kockázatot, azaz, hogy mennyi halálos kimenetű baleset engedhető meg egy-egy funkció meghibásodása következtében, hiszen ha teljesen hibamentes járműrendszerek előállítására törekednénk, nem lenne mivel közlekednünk.

Vegyük szemügyre az Európai Unió által megfogalmazott közlekedési balesetek statisztikáiból kiinduló éves bontásban ábrázolt halálos kimenetelű balesetek számát. Az 1.4 ábra grafikonján egy erőteljes csökkentési ütem előírásának igénye látható, amelyet még nem sikerült elérni annak ellenére, hogy folyamatosan szigorítják a közúti közlekedési szabályok megszegéséért járó szankciókat. Az újonnan forgalomba kerülő járműveket kötelezően alkalmazandó új biztonsági megoldásokkal szerelik fel, például: a jármű stabilitását javító Electronic Stability Program (ESP), illetve vezetést támogató ésvészhelyzet esetén beavatkozó Driving Assistant System (DAS) [23]. A műszaki

megoldások mellett megvizsgálták a balesetek okait is, amelyben kiderült, hogy a legtöbb, közel 90% alkalmával a baleset hátterében emberi tényezőre visszavezethető ok áll [60]. Megoldást a járművek műszaki színvonalának emelésében kívánják javítani.



1.3. ábra Előírt követendő trend az EU-ban [23]

A trendet betartani kötelezett autóiparnak lépést kell tartania az EU által előírt szigorú közúti baleseti statisztika javításával, amelyet jól definiált folyamataival tud gazdaságosan elvégezni [58]. Az informatika fejlődésével és a mesterséges intelligencia térhódításával a klasszikus járműiparon kívüli nagyvállalatok is bekapcsolódtak a fejlesztésbe, például az informatika területéről a közismert Tesla, illetve a Google elindította az első, emberi felügyeletet igénylő önvezető és elektromos autóját [39]. Az emberi tényező csökkentését önműködő járműirányítással valósítják meg, szenzor adat fúziót használva a forgalmi helyzetek felismeréséhez. Kritikus helyzetben azonban emberi beavatkozást kérnek ezek a rendszerek. Az emberi tényező csökkentésének szükségességét fogalmazta meg Sebastian Thrun is, a Google vezető fejlesztője is a TED 2011 konferencián [82].

A járművek megbízhatósága mind a mai napig kiemelt fontosságú, amit az 1.1 táblázat is mutat. A megbízható- és biztonságos működésen túl számos kényelmi funkció iránti igény is egyre nagyobb számban jelenik meg, amelyek a jármű hagyományos működtetésén túlmutatnak. Ezt a kérdést analizálta a Deloitte egy felmérésében, ahol az Y generáció (1982 – 1993 közötti népesség) igényét mérték fel a megvásárolandó jármű funkcióit illetően. Látható, hogy a korszerű fejlesztések mellett a vásárlók szükségletei is átalakulóban vannak [17].

Szempont	Nem fontos	Közömbös	Fontos
Minőség és megbízhatóság	18%	8%	75%
Üzemeltetés költsége	17%	14%	68%
Jármű design	19%	13%	68%
Üzemanyag takarékosság	20%	17%	64%
Teljesítmény	17%	21%	62%
Sokoldalúság, célszerű megoldások	19%	19%	62%
Márka	20%	20%	60%
Egyéb biztonsági rendszerek	27%	26%	48%
Technológia	25%	30%	44%
Környezeti hatás	31%	31%	38%

1.1. táblázat Fontossági szempontok egy új autó vásárlásakor [9]

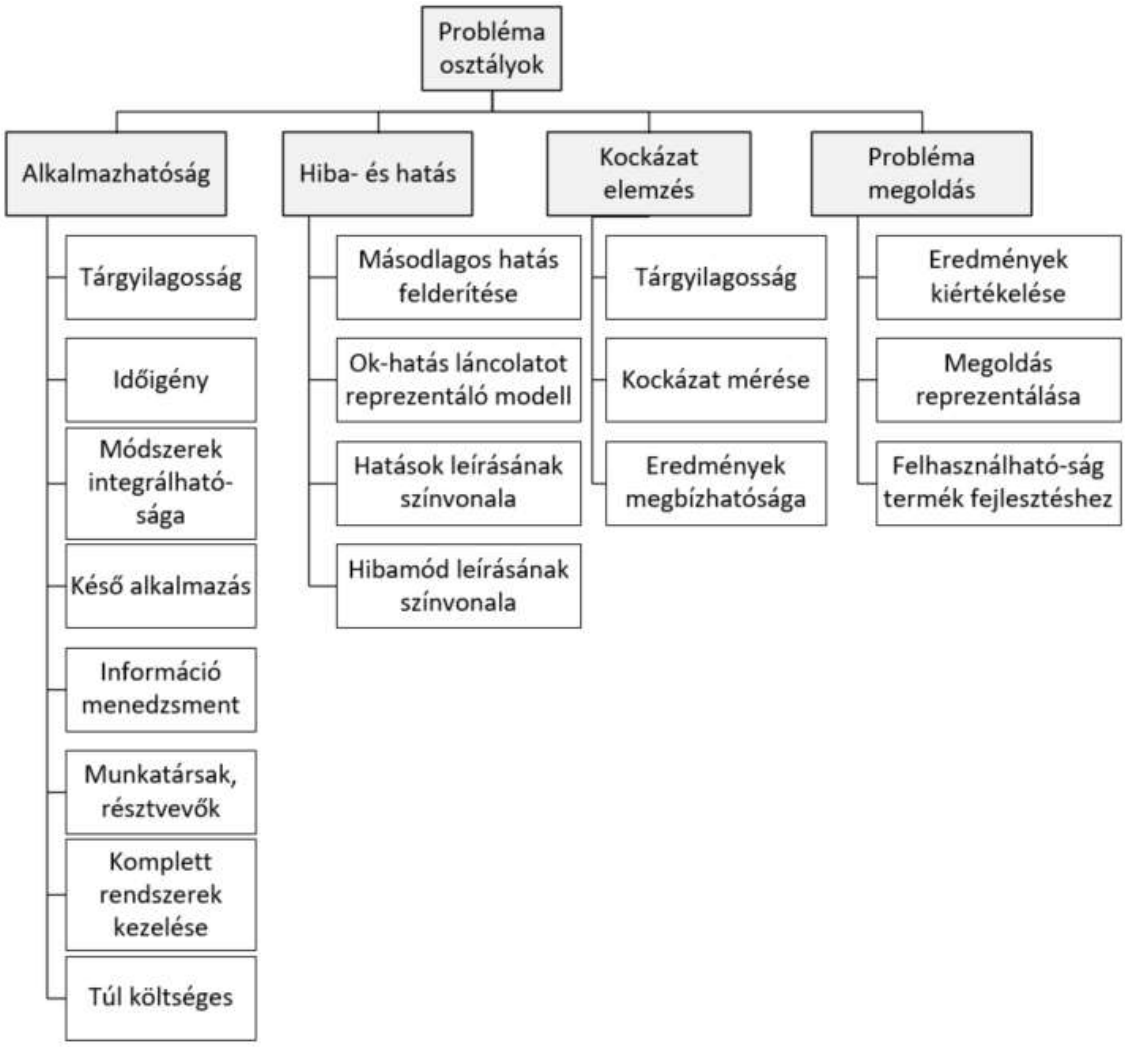
Megállapítható, hogy a jármű kezdeti funkciója, hogy egy adott úton megbízhatóan működve juttassa el az utasait már eléggé alapvető elvárás az új, kombinált hajtások bonyolultsága és gazdaságosságának, hatékonyságának növekedése ellenére. A szelekciót és eladhatóságot növeli leginkább az összetett működésű extra funkciók számának növekedése. A megvalósítandó luxus funkciók immár a vezetési élmény növelésén túl az utazás komfortjára is egyre jelentősebb súllyal jelennek meg. Ezen túl a gyártóknak és a beszállítóaiknak fel kell készülni a kombinálhatóságra, egyedi igények kiszolgálására is [81]. A gyorsan változó igények akár egy-egy fejlesztés újra felhasználására mind erősebb igényként fogalmazódik meg. Erre kell az előzetes megbízhatósági elemzésnek a fejlesztéssel együtt felkészülnie a járműiparban.

Jól látható, hogy az újonnan megjelenő telekommunikációs modulokat és funkcionális biztonságból jövő kockázatokat is szükséges belefoglalni az eddig elvégzett FMEA elemzésekbe.

1.2 FMEA a tudományos világban

Az FMEA használatával egy közös elemzésben kiértékelhető a sokszor eltérő szemléletű módszerekkel készített tervek kockázata. Alapvető gondolat, hogy egy rendszer funkcióit modellezve, azok lehetséges hibáit és a hibák hatásait írják fel a hiba forrásait, azaz a kiváltó okot megjelölve. A különböző szemléletű és igényű módszerek egy egységbe foglalása is megoldandó kérdéseket vet fel, amelyre mind akadémiai és ipari forrásokból jelennek meg tudományos közlemények. A megfelelő FMEA formanyomtatvány kitöltését és kiértékelését számos szoftver támogatja ugyan, de egy új modell felépítése a kezdetektől fogva már teljes mértékben a moderátor tapasztalatától függ [41]. Az FMEA témakörében megjelent publikációkat és szabadalmi bejegyzéseket vizsgálta át Sprefico és szerzőtársai az 1978 és 2016 közötti időszakban, kategorizálva azokat tartalmuk szerint. [75] A vizsgálat eredménye a 1.5. ábrán látható.

Mind az akadémiai úgy az ipari háttérből származó problémák témaköreinek eloszlása hasonló, a cikkekben taglalt témaköröket csoportosítva jelenítik meg. Az egyes témakörökben közöltek között van mennyiségi eltérés csupán (1.6 ábra). Mint az ábrákon látható, az alkalmazási kérdések igen előkelő helyre kerültek, amelyet az ok-hatás elemzése követ. A problémamegoldás hasonló helyet foglal el mind az ipari- úgy akadémiai területen, a kockázat elemzés témaköre az akadémiai körben jelentősebb (28%), szemben az ipari 9%-al. Az eloszlásból feltételezhető, hogy az ipari szereplők sokkal inkább összpontosítanak a módszer gazdaságossá tételére, mint annak más területen történő alkalmazására. Meglepő megállapítása az elemzésnek, hogy az elmúlt 5 évben több mint 200%-al nőtt a publikációk száma, szemben az elmúlt 25 évben összesen. Ez a növekedés mint az ipari, úgy akadémiai területen egyaránt jellemző, a legtöbb forrás Kínából származik [41].

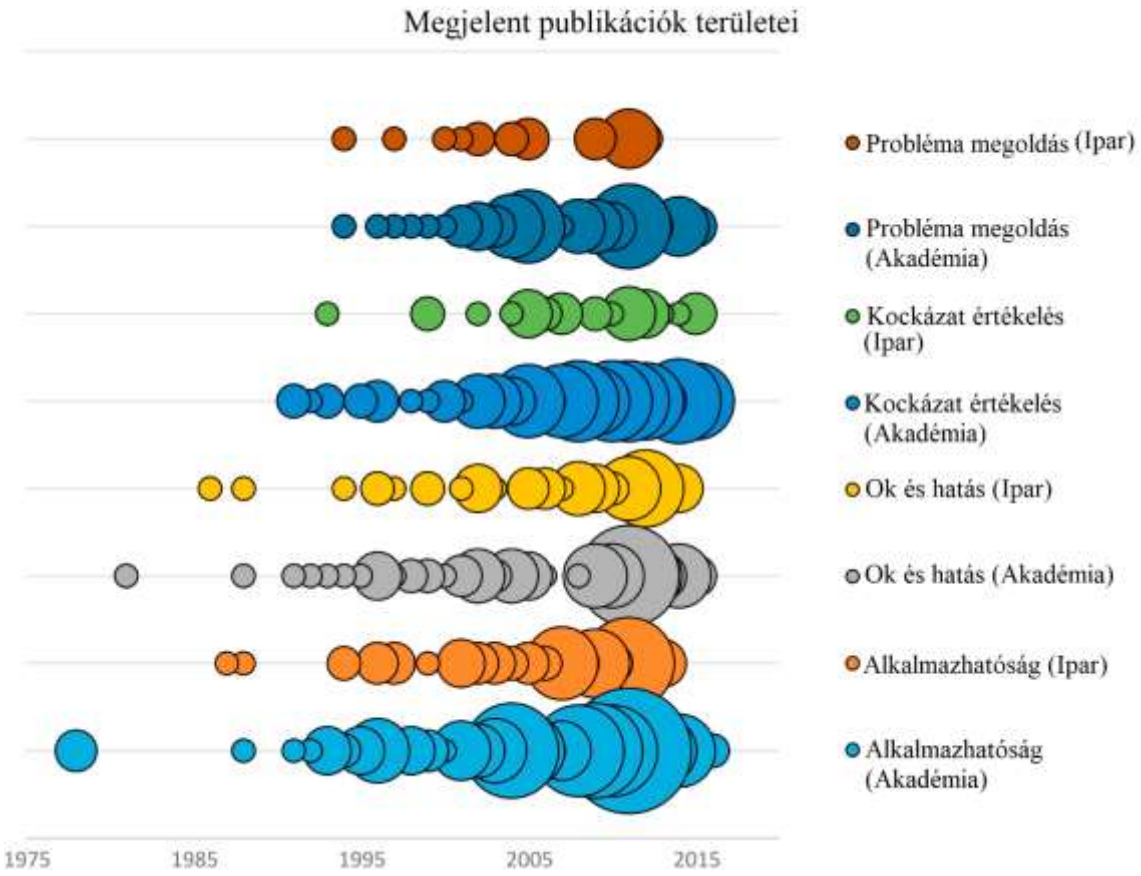


1.5. ábra Az FMEA témájú cikkekből felírt probléma osztályok [76]

A cikk által közölt megoldások időbeni mennyiségének alakulása látható a 1.6. ábrán, külön csoportokba bontva a megoldandó probléma osztály és a cikket közlő forrás szerint. Az ábrán is látható, hogy mind az ipar, úgy az akadémiai szereplők egyaránt jól érzékelik az 1.5 ábrán is látható probléma osztályokat; azonban az akadémiai szereplők főleg az elemzések információ tartalmára fókuszálnak, míg az ipari szereplők az automatizálhatóságon, az emberi tényező hatásának enyhítésén, illetve az ok-hatás reprezentálásának javításán és a hiba módok felismerésén dolgoznak [41].

Az akadémai oldalon egyre jobban megjelenik a Fuzzy elmélet alkalmazása a problémamegoldási területen, míg az analízis alapját képező csapat felépítését figyelmen kívül hagyják általában. A szerzők is megjegyzik, hogy nem jellemző az általános, égető

problémák megoldása, az erőforrásigény mérséklése vagy éppen az anyagjegyzék (Bill of Material) a kiértékelésének javítása [41].



1.6. ábra Az FMEA témájú cikkek megjelenései az adott témakörökben [77]

A dolgozat tartalmával kapcsolatos publikációk a rendszermodellezés tekintetében elsősorban a szoftver területen jelennek meg [61] [32], illetve a kockázatelemzés és kiértékelés témakörében [62]. Ezen témakör ismertetése az ide vonatkozó fejezetekben található.

A hibafa alapú rendszerelemzés alkalmazása szintén jelen vannak, de a vizsgálatot leginkább a biztonság, meghibásodási témakörök jelentették [13]. A gépjárműipari Funkcionális Biztonság (ISO 26262) előírásai kötelezővé teszik a hibafa elkészítését a magasabb kockázati szintű hibák esetén [36] [33]. Azt azonban nem részletezik, hogy egy követelményből eredő funkció hibájának felépülését vagy a kézzel fogható alkatrészeken alapuló meghibásodásokra készüljön-e az elemzés. Dolgozatomban a hibafa elemzést egy FMEA-ból kinyert adatok feldolgozására használom fel érzékenység vizsgálatára.

1.3 Alkalmazott kutatási módszerek

A kutatásom célkitűzése az autóipar működési szabványai, szabályozásai által előírt, kötelezően használandó módszerek alkalmazási gyakorlatának optimalizálása és jobbítása formális módszerekkel a termékbiztonság- és megbízhatóság előzetes becslésének érdekében. Amint az ismertetésre került, a járműfejlesztés a vásárlótól kapott követelményeket funkciókba csoportosítva vizsgálja elsősorban. Ezek működését meghibásodási kockázatok megismerésével kívánja egy társadalmilag és üzletileg is elfogadott kockázati szintre optimalizálni egy-egy intézkedéssel vagy módosítással. Az egyre felgyorsuló gazdasági környezet és ezen keresztül a vevői igények változása jelentős kihívásokat generál az iparági szereplők számára folyamataik optimalizálása és gazdaságos működése tekintetében. Az előírt és kötelezően alkalmazandó hibamód és -hatáselemzés egy nagyon időigényes kockázatelemzési eszköz, amelyben egy rendszer modellezésén keresztül vizsgálják meg az egyes funkciók által jelenlévő kockázatokat. A megoldandó probléma egyrészről az egységes, összefoglaló rendszermodell felállítása, amely magába foglalja az elektronikus hardver, mechanikai komponensek és szoftver összetevők közös modellben elemzését. Másrészről a kockázatok és összetevőik tartalmának és súlyának helyes értelmezése. Az elemzési módszerek sajnos nem nyújtanak könnyű áttekinthetőséget a kockázatok tartalmára vonatkozóan. Ezért egy könnyen áttekinthető és értelmezhető grafikus reprezentáció kidolgozása a célom, amely a rendszer gyengepontjaira, azaz az érzékeny pontokra enged következtetni.

Végül a számba vehető hibák kialakulásának további elemzését vizsgálom meg, mivel az FMEA egy-egy hibát definiál és elemez végig a rendszerben, addig a hiba felépülését a hibafa módszer analizálja. Egy elkészült hibafa azonban további elemzésre szorulhat, amely a hibát felépítő elemi események legkritikusabb kombinációjának vagy részhalmazának a megtalálására fogalmaz meg kihívásokat. Ebben segít az érzékenységvizsgálat, amely a megfelelő elemek azonosításával javítja a rendszer robusztusságát, hiszen ismertté válnak azok az elemi események, amelyek bekövetkezésével a rendszer leginkább instabillá vagy hibássá válhat.

A létrejövő eredmények a megbízhatósági vizsgálatokat és a termékfejlesztést is támogatják az előzetes termékanalízissel. A megfelelő tesztstratégiával meggyőződhetünk, hogy mely tesztek szükségesek akár egy regresszióhoz[1] vagy a termék fejlesztési

[1] regressziós teszt: minden egyes verziónál ezek azok a tesztek amivel meggyőződhetünk, hogy a változtatás nem rontotta el az adott funkció stabilitását, előírt működését

életciklusában egyszeri tesztelés futtatásához. A jól megválasztott monitorozó és megelőző eljárásokkal feltehetően a rendszer megfelelően ellenáll a működést befolyásoló váratlan hatásoknak.

A prezentálhatóvá váló grafikusan ábrázolt adatok betekintést adnak a rendszer aktuális állapotába, amely a specialistákon túl a döntéshozó menedzsereknek nyújtanak összehasonlítható információt. A fejlesztők munkáját tovább könnyítheti a tematikus kérdések alkalmazása, felkészülési stratégia és a formanyomtatványok alkalmazása. Ezek mind az emberi tényezőből eredő hibák csökkentésére szolgálnak, illetve a kapacitás gazdaságos kihasználásának növelésére. A disszertációmban egy-egy gyakorlati példát is bemutatok, amelyek az adott módszer alkalmazásai.

Disszertációm az alábbi fejezetekből áll: A 2. fejezetben röviden ismertetem a két előírt módszertan (FMEA, FTA) főbb jellemzőit, alkalmazási gyakorlatát. A 3. fejezetben az egységesített rendszermodellezés kerül bemutatásra az egyes diszciplínák (hardver, szoftver, mechanika) elvárásait ismertetve. A 4. fejezetben a hibafa elemzés érzékenységvizsgálati módszerének egy alkalmazása kerül bemutatásra a rendszert leginkább veszélyeztető elemi hibák kiemelésére. Az 5. fejezetben az általam kidolgozott hierarchikus FMEA-t rendszerezési modellt ismertetem. A 6. fejezetben az FMEA érzékenység vizsgálatát és a kockázati számok értékelésének finomítását végzem el, illetve a hibafa- és hibamód és -hatás elemzés érzékenységi vizsgálatát hasonlítom össze.

2 A TERMÉKBIZTONSÁG BECSLÉSE

Sok esetben egy termék megbízható és biztonságos működésén hasonló fogalmat értünk, azonban mérnöki szempontból szét kell választanunk. Megbízhatónak tekinthető egy rendszer, ha egy fellépő hiba nem képes befolyásolni az egész rendszer működésének stabilitását. Az MSZ IEC 50(191) szabvány meghatározása alapján [54]: „A megbízhatóság gyűjtőfogalom, amelyet a használhatóság és az azt befolyásoló tényezők, azaz a hibamentesség, a karbantarthatóság és karbantartás-ellátás leírására használnak.” Megbízhatóság mértéke számszerűen kifejezhető általában a hibátlan, üzemszerű működési valószínűségével. Biztonságosnak tekinthető egy rendszer, ha nem okoz emberi egészséget, életet veszélyeztető eseményeket, illetve gazdasági vagy környezeti károkat. A termékfejlesztési kockázatok azonosításának helyét a követelményelemzéshez helyezi Shaojun Li [45] egy jól ismert minőségirányítási tételként, miszerint egy hiba kijavítása minél korábban történik egy fejlesztés életciklusában, annál hatékonyabb és gazdaságosabb azt kijavítani [56]. A biztonságos, megbízható működés fenntartása érdekében a gépjárműipari rendszerek egyes funkciójával, elemével szemben szigorúbb előírásokat fogalmaznak meg a kockázati szintjük alapján [1]. A kockázatok azonosítására azonban modellezni és értékelni szükséges a rendszert, amelynek eredményével olyan intézkedéseket vezetnek be, amelyek csökkentik a hibák következményeit vagy előfordulását, illetve növelik az észlelhetőségét. Ritkábban előfordulhat ugyanakkor az adott funkció bővítése vagy újra tervezése is.

A fejlesztés első lépéseinél elkezdődik a járműrendszer funkcióinak vizsgálata, kockázatelemzési módszerek alkalmazásával – deduktív vagy induktív módon. A funkció kockázatelemzési módszerei általában három paraméterből számított becslést alkalmaznak. E három a súlyosságra (mekkora veszteséget okoz az esemény), előfordulási valószínűségre (adott populációból mennyire teljesül, mennyire gyakran fordul elő), valamint az észlelhetőségre, detektálhatóságra vonatkozó paraméter (könnyen- vagy nehezen észlelhető és azonosítható). Ezen három paraméter szorzata a kockázati szám, ami alapján lehet viszonyítani, rangsorolni az eseményeket. Ilyen módszert alkalmazunk a hibamód és –hatás elemzés (FMEA), veszély- és kockázatelemzés (HAZOP) eleljárásokban is. Ugyanakkor jellemző egy adott hibaesemény mélyebb megismerésére törekvés, kialakulásának szabályszerűségét logikailag leírni az egyes kapcsolatok feltárásával. E kapcsolatok

átmeneteit egy-egy valószínűségi értékkel jellemezik, az adott esemény bekövetkezésének megismerése a cél (például: hibafa (FTA), eseményfa (ETA)).

Fontos megjegyezni, hogy a kockázati elemzésnek mindig egyszeres hiba bekövetkezését kell vizsgálnia, mert egy második hibával már nagyobb eséllyel válhat irányíthatatlanná a rendszer, átugorva a biztonsági állapotot (safe state). Másrészről egy összetett hiba kombináció elemzésével nagyon hamar követhetetlenné válik az elemzés. Kiemelendő még, hogy teljesnek (complete), egységesnek (consistence) és helyesnek (correct) kell lennie [43].

2.1 A Hibamód és -hatás elemzés kialakulása és főbb jellemzői

A hibamód és -hatás elemzés (FMEA) a National Aeronautics and Space Administration (NASA) által kifejlesztett módszertan, amelyet az űrprogram elektronikus eszközeinek megbízhatósági elemzéséhez fejlesztettek ki 1960-as években. Ez fejlesztés az Amerikai Hadsereg fejlesztésére épül, amelyet az 1949-ben megjelent MIL-P-1629 dokumentumára épülve fejlesztettek. A hadsereg átdolgozta a dokumentumokat 1980-ra, amelyek MIL-STD-1629A [51] és MIIL-STD-785B dokumentumokban jelentek meg[52]. Végül az autóipar is alkalmazza, a Society of Automotive Engineers (SAE) 1967-ben [71]. Mára minőségbiztosítási rendszerek hivatkozzák meg például: QS-9000[67], ISO 9004[22], IATF 16949[37], stb.. [48]. A módszertant más ágazatok is alkalmazzák, például: háztanúsításban (LD 5.2 szabvány) [7], vagy az egészségügyben az amerikai The Joint Commission által akkreditált intézményekben egy-egy nagykockázatú folyamat kiválasztására [27]. Magyarországon az MSZ EN 60812:2006 [53] szabvány ismerteti „A rendszer-megbízhatóság elemzési módszerei. A hibamód- és hatáselemzés (FMEA) eljárása” címmel [53].

Már a koncepció fejlesztési szakaszban is támogatást nyújt a költségek optimalizálásában, amely a teljes termékfejlesztési életciklust (fejlesztéstől a gyártásig) lefedi. Bármilyen terméket érintő műszaki kockázat felmérésére is hatékony eszköz induktív módszerként alkalmazva. Eredményei felhasználhatóak más módszertanok számára is, például a hibafa elemzéshez vagy az autóiparban kötelezően alkalmazandó „state-of-the-art”

szint teljesítését biztosító funkcionális biztonsági elemzésben (ISO 26262) használatos HARA[2]-ban.

Ugyanakkor a HARA eredményei is nyújtanak bemeneti adatokat az FMEA számára. Alkalmas egy megfelelő modellezés esetén több szakmai terület ismeretének azonos szempontok szerinti elemzésére, azok logikai összekapcsolására és egy átfogó jellegű, áttekintő kiértékelésére. Egy vállalaton belül a tervezőktől kezdve a logisztikán át egészen a gyártásig nyújthat információt az adott területet érintő feladatok kockázatairól egy megfelelő mélységben kielemzett termék változtatási igényének azonosításában és feldolgozásában is. Az elemzést emberi produktumként végzik el, amely magában hordozza az egyik gyenge pontját is, az emberi (humán) faktortól való jelentős függést. Ebből következik, hogy a modellezés hatékonysága, kidolgozottsága és eredményessége nem egységes. A résztvevők eltérő ismerete és látásmódja miatt az adott szakterület képviselői mellett a megbeszéléseket egy, a módszertanban járatos moderátor vezeti. Ez azonban egy jól körülhatárolt rendszerben sem jelent garanciát a sikerhez, mert magát a rendszert egyben még így is nehéz átlátni, illetve egy-egy pont elemzése sok kapacitást igényel. Fontos kiemelni, hogy egy termék funkcióinak kockázati elemzésére hatásosan használható a módszertan, de könnyen válhat túltervezetté is. Ezért szükséges az FMEA értelmezését és paramétereit megfelelően kezelni, a megbeszéléseket lehetőségekhez képest sematizálni [25].

2.2 A Hibamód és -hatáselemzés alkalmazása

Az elemzés egy formanyomtatvány szisztematikus kitöltését jelenti, ahol a termékről egy leíró jellegű analízis készül. A döntéshozók által jóváhagyott, az iparágban használatos minőségirányítási rendszer előírása alapján alkalmazhatnak egy szintű- vagy egymásra épülő, többszintű (kaszkád) elemzést. Egy-egy rendszer lentről-felfelé (bottom-up) haladva kerül analizálásra elméletileg, amelyet lehet funkciókra, vevői elégedettségre vagy az alkatrészekre támaszkodva elemezni. Itt is az egyszeres hibákat kell kiértékelni attól függetlenül, hogy valójában bekövetkezik-e vagy sem? A vizsgálat eredménye a rendszer funkcióinak, elemeinek rangsorolása kockázat szerint [78]. Az előírások alapján kerül alkalmazásra egy közösen alkalmazott kiértékelő katalógus (ranking catalogue). Ez a katalógus egy-egy szabvány vagy ajánlás által javasolt szempontrendszer szerinti pontozás, azonban egy vállalatnak a saját tapasztalataikkal kiegészített belső

[2] Hazard And Risk Assessment: Az elemzés meghatározza a biztonságkritikus rendszer egy-egy adott funkciójához alkalmazandó biztonsági szintet. Az ISO26262, ISO25119/DIN EN 16591 egyaránt megtalálható, ez által a személygépjárművek és a mezőgazdasági gépek elemzésénél is alkalmazzák [83].

használatú katalógus kidolgozása és alkalmazása jellemző. Általánosan elterjedt az autóiparban használt SAE J1749 szabvány [71] alkalmazása, de a VDA[3] és AIAG[4] ajánlásai is jelen vannak hasonló tartalommal.

A kaszkádba rendezett elemzést külön-külön szinteken, eltérő tárgyú és mélységű logikai elemzésre alkalmazzák. Az adott szintek értelmezésében eltérés van az autóipari szabványok között. Az egyik ilyen a VDA szerinti rendszer (system), konstrukciós (design) és gyártási folyamat (process) FMEA [86], míg a AIAG külön ír fel konstrukciós (design), és gyártási folyamat (folyamat) FMEA-t [29]. Ezek általános összekapcsolódását, egymásra épülését a hiba-hatás, ok-hiba mód-effekt, mód-hatás láncolatok alkotják [48].

Ez azt jelenti, hogy egy felsőbb szinten megfogalmazott elem kerül örökítésre (mintegy lemásolásra) egy- vagy több szinttel lentebbi helyekre a hozzá tartozó pontértékkel együtt. Ez a megközelítés a felülről-lefelé (top-down) elvet követ, szemben az elméleti leírásokkal. Véleményem szerint szükséges a kockázatok rögzítése ilyen módon, hogy egyszer szerepeljen áttekinthető módon. Így lesz egy rendszerben az adott hibahatásnak azonos elnevezése, pontszáma és értelmezése. Ezt követően azonosíthatóak az egyéb intézkedést igénylő kritikus pontok.

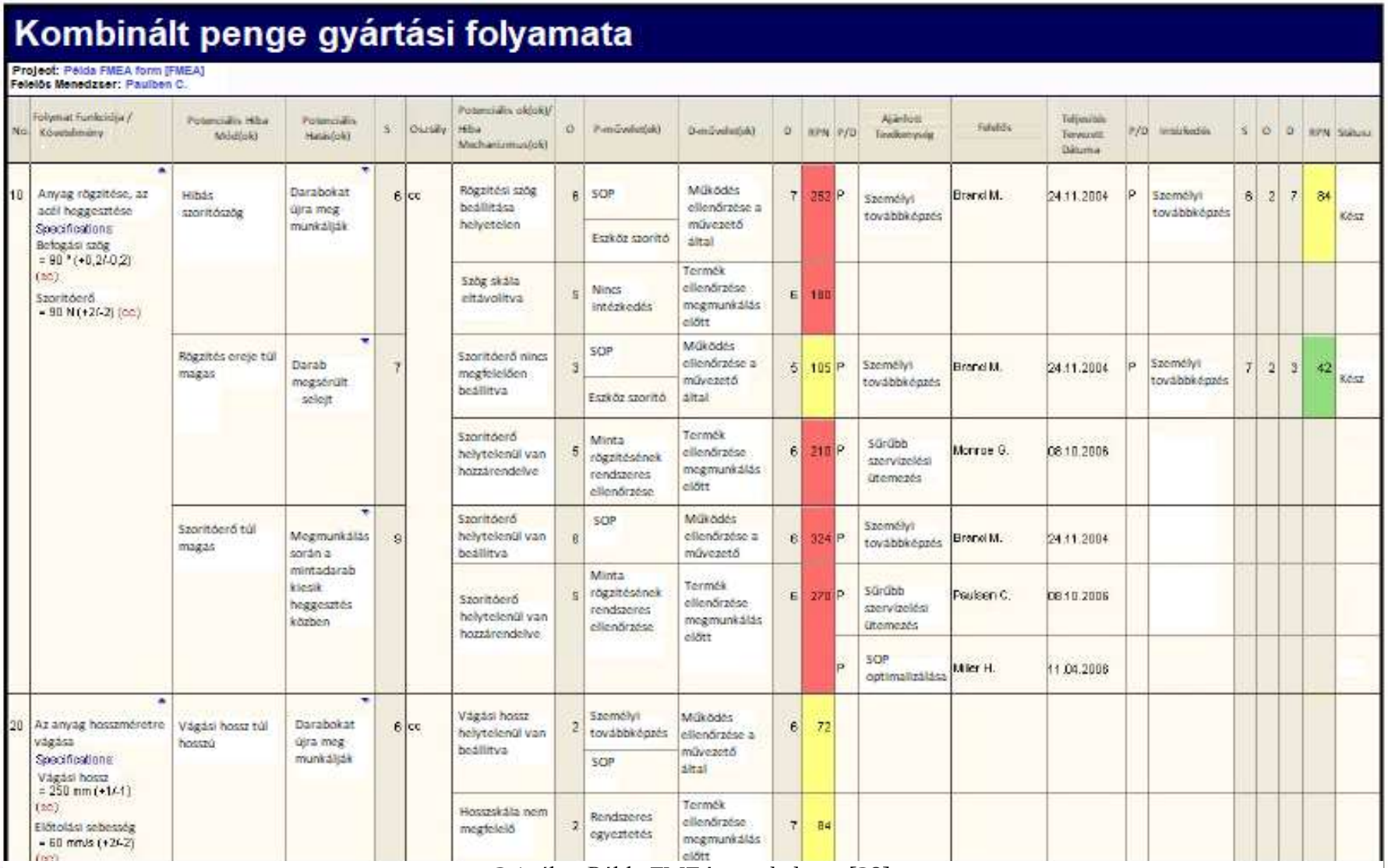
Az FMEA kiértékelése három paraméter alapján történik. Az első paraméter segítségével az adott elem hiba hatásának súlyossága (S-Serverity), majd az azt kiváltó ok előfordulásának gyakorisága (O-Occurence), illetve az észlelhetősége (D-detection) kerül pontozásra a korábban említett értékelési katalógus felhasználásával. Az előfordulási paramétert a korai fejlesztési fázisban elég nehéz megítélni, így korábbi tapasztalatok alapján becsülik meg. Az adott hibahatáshoz tartozó észlelhetőség paramétert egy monitoring rutin hatékonysága vagy egy mérnöki folyamat előírásának ismeretében értékelik ki [15].

[3] Verband der Automobilindustrie e.V.: A német autóipari gyártók és beszállítók szövetsége. A központja Berlinben van, szabványokat, és ajánlásokat tesznek közzé. [87]
[4] Automotive Industry Action Group: Észak-amerikai Autóipari Szövetség, amelynek tagjai között vannak az amerikai gyártók mellett a Japán autógyártók is. Szabványokat, ajánlásokat dolgoznak ki és oktatásokat szerveznek. [4]

Az FMEA készítése és fenntartása egy folyamatos, véget nem érő munkát jelent. A túlságosan magas kockázatokat javító intézkedések meghatározásával szükséges csökkenteni. Másrészről elvárás, hogy „élő dokumentum legyen” azaz mindig az éppen érvényben levő rajzokat, terveket és állapotokat tükrözze a termékkel kapcsolatban. Az elemzés segítésével egy termék minőségi értékelése válik lehetővé elsősorban műszaki kockázatok csökkentésére. Segítségével láthatóvá válik egy termék megbízhatósága, biztonsága, hiszen a kockázatokon keresztül az adódó hibákra, azok kezelésének színvonalára és átgondoltságára is következtethetünk. Hátrányai között szerepel a nehezen becsülhető munkaerő kapacitási- és időigénye, hiszen egy-egy komponens lehet, hogy több szakértőt igényel, illetve a megfelelő részletesség megtalálása elhúzódó megbeszéléseket eredményezhet. A módszertan helyes és hatásos alkalmazása ellensúlyozhatja a főbb negatívumokat, ha sikerül újra felhasználható- illetve könnyen követhető rendszermodellt megalkotni. [1]

Egy formanyomtatványi példa látható a 2.1 ábrán, ahol az oszlopokban szereplő adatok sorra a következők:

- Funkció: a kitöltők megállapítása alapján a rendszer tagolódásának megfelelően, felveszik a funkciót az adott szinthez.
- Hibamód: szakértők bevonásával felderítik, hogy a korábban felírt funkció miként hibásodik meg.
- Hibahatás: a már felírt hiba lehetséges hatását írják fel, azaz mi a látható hatása a rendszeren.
- Ezt a hibamódot pontozzák a hiba következménye alapján súlyossági számmal (S).
- Hiba okának meghatározása. Ez az ok (cause), amely kiváltja a meghibásodást.



Kombinált penge gyártási folyamata

Projekt: Példa FMEA form [FMEA]
Felelős Menedzser: Paulsen C.

No.	Folyamat Funkciója / Követelmény	Potenciális Hiba Mód(ok)	Potenciális Hatás(ok)	S	Osztály	Potenciális ok(ok)/ Hiba Mechanizmus(ok)	O	Prev.Control(ok)	Det.Control(ok)	D	RPN	P/D	Ajánlott Intézkedés	Felelős	Tervezett Befejezés Dátuma	P/D	Intézkedés	S	O	D	RPN	Státusz
10	Anyag rögzítése, az acél hegesztése Specifications: Befogási szög = 90 ° (+0,2/-0,2) (cc) Szorítóerő = 90 N (+2/-2) (cc)	Hibás szorítószög	Darabokat újra meg munkálják	6	cc	Rögzítési szög beállítása helytelen	6	SOP Eszköz szorító	Működés ellenőrzése a művezető által	7	252	P	Személyi továbbképzés	Brand M.	24.11.2004	P	Személyi továbbképzés	6	2	7	84	Kész
						Szög skála eltávolítva	5	Nincs intézkedés	Termék ellenőrzése megmunkálás előtt	6	180											
		Rögzítés ereje túl magas	Darab megsérült sérült	7		Szorítóerő nincs megfelelően beállítva	3	SOP Eszköz szorító	Működés ellenőrzése a művezető által	5	105	P	Személyi továbbképzés	Brand M.	24.11.2004	P	Személyi továbbképzés	7	2	3	42	Kész
						Szorítóerő helytelenül van hozzárendelve	5	Minta rögzítésének rendszeres ellenőrzése	Termék ellenőrzése megmunkálás előtt	6	210	P	Sűrűbb szervizelési ütemezés	Monroe G.	08.10.2006							
		Szorítóerő túl magas	Megmunkálás során a mintadarab kicsik hegesztés közben	8		Szorítóerő helytelenül van beállítva	8	SOP	Működés ellenőrzése a művezető	6	324	P	Személyi továbbképzés	Brand M.	24.11.2004							
						Szorítóerő helytelenül van hozzárendelve	5	Minta rögzítésének rendszeres ellenőrzése	Termék ellenőrzése megmunkálás előtt	6	270	P	Sűrűbb szervizelési ütemezés	Paulsen C.	08.10.2006							
												P	SOP optimalizálása	Miller H.	11.04.2006							
20	Az anyag hosszméretre vágása Specifications: Vágási hossz = 250 mm (+1/-1) (cc) Előtolási sebesség = 60 mm/s (+2/-2) (cc)	Vágási hossz túl hosszú	Darabokat újra meg munkálják	6	cc	Vágási hossz helytelenül van beállítva	2	Személyi továbbképzés SOP	Működés ellenőrzése a művezető által	6	72											
						Hosszskála nem megfelelő	2	Rendszeres egyeztetés	Termék ellenőrzése megmunkálás előtt	7	84											

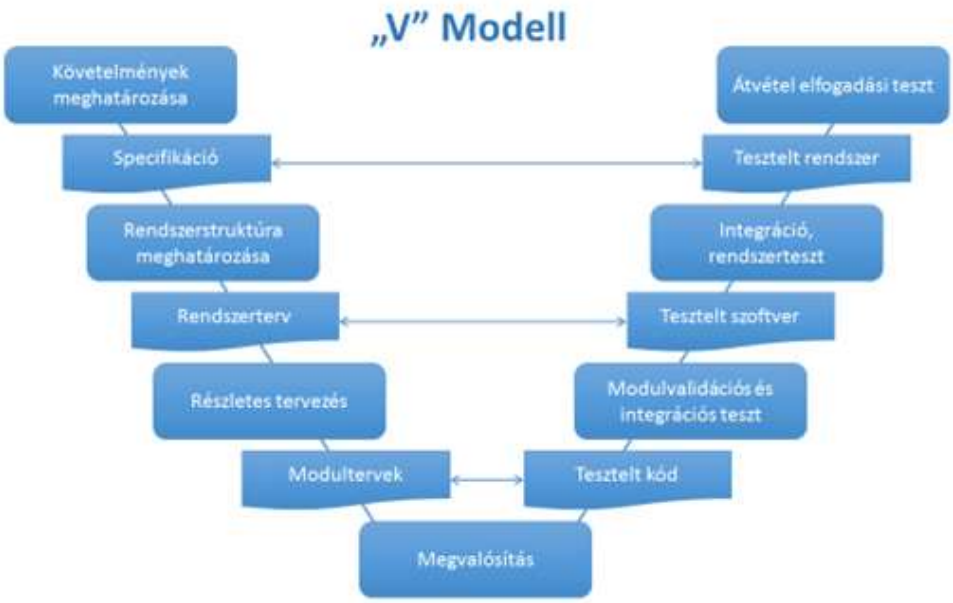
2.1. ábra Példa FMEA munkalapra [28]

- A meghibásodás előfordulását (O) felírva – láthatóvá válik, milyen gyakran fordulhat elő ez a hiba ok.
- A hiba bekövetkezésének elhárítása érdekében lehetséges alkalmazni megelőző vagy észlelhető akciókat. A preventív akció segítségével a fejlesztés során kerül megakadályozásra az adott hiba, míg a detektív elem segítségével az esetlegesen bekövetkező hiba észlelése kerül osztályozásra – mennyire hatékony.
- A felírt pontszámok szorzata adja a kockázati prioritási számot, azaz a Risk Priority Number (RPN)-t, amely számítása RPN=S·O·D szorzatából adódik, a kockázat rangsorolásra használt mutatószám.

Kiértékelésekor a RPN számok alapján állapítják meg az adott funkció, elem kockázati szintjét. Ha valamelyik meghalad egy előzetesen definiált kockázati szintet (RPN határértéket), akkor szükséges intézkedéseket tenni annak a kockázati szám csökkentésére. Ilyen lehet például egy hatékonyabb mérés, észlelés, mérési elemzés, monitorozás, stb.) hozzáadása. Ha bizonyítottan sikeres a jobbításra kiírt akció, akkor a súlyossági (S) érték kivételével módosítható az előfordulás (O) és észlelhetőség (D) számok – alacsonyabb RPN értéket elérve.

2.3 Az autóiparban alkalmazott tesztelési folyamat és az FMEA kapcsolata

Az autóipari fejlesztés folyamata a biztonságkritikus háttere miatt a V modellen alapuló fejlesztést követi, az egymásra épülő munkacsomagok a 2.2 ábrán látható. Egy fejlesztési ciklus a tematikus követelmény lebontással indul egészen a fejlesztésig, majd a lépésenkénti összeintegrálással és teszteléssel együttesen haladva jut el a termék verifikációjához. Jellemző, hogy az egyes feldolgozott szint lezárása után indulhat az előző lépést részletesebben kidolgozó, következő munkafolyamat (horizontális sorrend). Az egyes szinteken keletkező előírások ellenőrzése jellemzi (vertikálisan) a V modell jobb oldalát az integrálás közben. Ebből eredendően, a kialakult követelmények lebontása, majd a fejlesztés és végül a tesztelés vízeséssszerűen követik egymást, ezért is nevezték a V modellt megelőző fejlesztési modellt vízesés modellnek [22].



2.2. ábra V-modell alkalmazása a fejlesztésekben [3]

Az egyes tesztelési szintek meghatározásai is az alábbi elveket követik, a tesztelés mélységét pedig az iparági biztonsági szabványok előírásai alapján végzik el. Elsődlegesen követelményeken alapuló teszteléseket végeznek, de figyelembe kell venni a szabványok által előírt vizsgálatokat is. Az előzetes kockázatelemzésből keletkező feladatok szintén deklarálhatnak végrehajtandó feladatokat. Itt adódhat egy kapcsolódási pont az FMEA-hoz, mert mint kötelezően alkalmazandó induktív elemzési módszertant, az ISO 26262 Funkcionális biztonsági szabványon [36] túl az iparági szabvány, az ISO-TS (újabban IATF) 16949 is előírja. A fejlesztésben alkalmazott Advanced Product Quality Plan (APQP)

(*magyarul minőségtervezés)* [6]) egy minőségtervezési aspektusként létrehozandó dokumentumot a Control Plant-t említi, amelyet szintén támogat az FMEA-ból jövő elemzés [16]. A mérnöki tervezés során alkalmazott kockázatbecslés segítségével meg tudják becsülni a minőségügyi- és fejlesztési kockázatokat. Az így készült FMEA elsődlegesen a fejlesztendő termék adott funkciójának meghibásodására fókuszál és azt értékeli ki, figyelembe véve a meghibásodás észlelhetőségének képességét egy rendszer működése közben. A projekt számára nem megengedhető nagyságú kockázatokat csökkenteni kell egy-egy megfogalmazott akcióval, majd kiértékelni annak eredményét. Erre általában teszteket vagy tervbeli módosításokat írnak elő, amelyek hatékonyságának eredményéről újabb mérésekkel, tesztekkel bizonyosodnak meg és rögzítik ezek hatását az FMEA-ban. Ugyancsak, mint terv – követelmény – kockázat között kapcsolatot létesítő eszköz megfelelő kidolgozás esetén támogatást nyújt a gyenge pontok azonosításában és rangsorolásában. Ezek a tesztelés ütemezésében minimum tesztelendőnek definiálhatók a Teszt Menedzser döntését megkönnyítve.

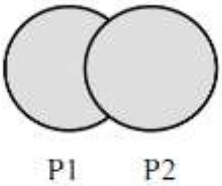
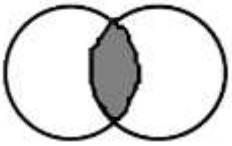
2.4 A hibafa elemzés kialakulása és főbb jellemzői

A hibafa analízist (FTA) a Bell Telefon Labor fejlesztette ki 1962-ben az Amerikai Légierő megbízásából, a Minuteman rakétarendszerél alkalmazta [11]. A mai formája egy NASA tanulmányba került összefoglalásra 1994-ben [30] [11]. Azóta széles körben alkalmazzák megbízhatósági- és rendszerbiztonsági elemzésekben [2].

Egy-egy rendszer analizálását lehet funkciókra, vevői elégedettségre vagy az alkatrészekre támaszkodva elvégezni. Itt is az egyszeres hibákat kell kiértékelni attól függetlenül, hogy valóban bekövetkezik-e vagy sem. A vizsgálat eredménye egy hiba kialakulási mechanizmusának megismerése, a hiba bekövetkezésében legjelentősebb elem vagy elemek azonosítása.

Az elemzés felépítése együttesen alkalmazza a Boole-algebra szabályait és szimbólumait, építőelemeit és a gráfelméletet. Egy felülről-lefelé (top-down) haladó elemzés, a legfelső (TOP) főeseményből indul ki, haladva a logikai kapcsolatokon keresztül egészen az elemi eseményekig. Megkülönböztetünk közbenső és elemi eseményeket, amelyek közötti átmenetet egy valószínűségi értékkel írhatunk le. Az egyes logikai kapukon áthaladást úgynevezett terjedési egyenlettel írhatunk le. Ezek az egyenletek a logikai kapukból levezetett matematikai egyenletrendszert alkotnak, amely számítások segítségével

a kimeneten jelentkező valószínűség kiszámítható. A 2.3 ábrán bemutatom a legismertebb logikai kapukat, azok szemléltetését Venn diagrammon, illetve a hozzájuk tartozó terjedési egyenletet [1].

Szimbólum	Név	Venn diagram	Terjedési egyenlet
	VAGY kapu		$P_T=P_1+P_2-P_1P_2$
	ÉS kapu		$P_T=P_1*P_2$

2.3. ábra Leggyakarabban használt logikai kapuk [1]

2.5 A hibafa alkalmazása

A hibafa alkalmazásának célja, hogy a vizsgált rendszer egy (és csakis egy) meghibásodás okát részletesen feltárjuk. A meghibásodást ismerve, annak ismert vagy ismeretlen okai után kutatva. Általános cél a logikai hálózat felépítésén keresztül a valószínűségi értékek által megbecsülni a csúcsesemény bekövetkezési valószínűségét számszerűsítve, illetve megállapítani, hogy az elemi események milyen súllyal befolyásolják a csúcsesemény létrejöttét és milyen állapotokon, feltételeken keresztül (milyen könnyen) juthatunk el oda. Az ilyen gyenge pontok azonosításához egyrészről vágatokat (cut set), illetve útvonalakat (path set) lehet létrehozni. A vágatok olyan minimális, elemi eseményeket tartalmazó halmazt írnak le, amelyek együttes bekövetkezésével a csúcsesemény biztosan bekövetkezik. Azonban, ha a halmazból egyetlen elemi esemény kivételével mind előállna a csúcsesemény biztosan még akkor sem következik be. Ezzel azonosítva a csúcsesemény bekövetkezési lehetőségeit, megtalálva az üzemszerű működést veszélyeztető hibákat, amelyek szerkezeti és minőségi tulajdonságokra is hatással lehetnek. Ezzel szemben az útvonalak (path set) az olyan elemi események halmaza, amelyeknél ha egyetlen egy elemi esemény sem következik be a halmazból – akkor biztosan nem fog bekövetkezni a csúcsesemény sem. Ez diagnosztikai mérésekhez, más területekhez

kapcsolódásban, költségbecslésben nyújthat támogatást. Clemens megjegyzi, hogy a path set megtalálásában segítséget nyújt a cut set ismerete, ha minden „ÉS” kaput „VAGY” kapura, minden „VAGY” kaput „ÉS” kapura cserélünk, majd a de Morgan dualitás elméletének felhasználásával átírjuk [11] [1].

Abonyi megemlíti, hogy közbenső események (intermediate event) definiálása is lehetséges, amelyek bekövetkezési valószínűsége nem ismert ugyan, de „az elemi eseményekkel azonos módon kezelendő. Közbenső események meghatározásával hierarchikus hibafa-rendszert alakíthatunk ki.”[1] A Boole-algebrán felül alkalmazható az úgynevezett transzfer kapu vagy transzfer esemény. Ez a hibafa tagolásán túl egy esemény több helyen való feltüntetését is elősegíti. A bekövetkezési valószínűségeket kvantitatív módszerekkel célszerű meghatározni, szakértők bevonásával. Amennyiben nem sikerül pontos értéket megbecsülni egy elemi eseményre, úgy használható az alsó- és felsőkorlát logaritmikus átlagából számított exponenciális értéke. Jellemző, hogy nem rendelünk értéket az adott átmenethez vagy csupán egy becslés áll rendelkezésre. [11].

A hibafa elemzés előnye az egy-egy hiba (csúcsesemény) kialakulásához vezető hibakombinációk kivizsgálásában rejlik. Az adott elemi hiba vagy hibakombinációk kialakulásáról, bekövetkezési esélyéről nagyságrendi tájékoztatást is szolgáltat a valószínűségi változókon keresztül. A halmazdefiníciók segítségével akár döntést támogató információk is kinyerhetők, akár diagnosztikához vagy gazdasági kimutatásokhoz, stb. is. Hátránya, hogy egy elemzés csak egy csúcseseményt képes kielemezni, komplex rendszerben ezért egy időben több, párhuzamos elemzést kell elvégezni. Valószínűségi számok kis mértékéből adódóan nő a számítási kapacitás. Egy logikai kapuhoz csak független elemi események kapcsolódhatnak, az elemi események valószínűségének konstansnak és jól meghatározhatónak kell lenniük [1].

2.6 Következtetések, ajánlások

Ebben a fejezetben bemutattam az autóipari fejlesztésben általánosan és kötelezően alkalmazott két elemzési módszertant a fejlesztési kockázat megbecsülésére. Mint látható a hibamód és -hibahatás elemzés (FMEA) mintegy átkarolja az egész fejlesztési folyamatot a logisztikától a gyártásig teljesen. Alkalmazására a minőségbiztosítási rendszer szabványi előírása miatt van szükség, azonban az elemzés által készült kockázat becslés eredménye, mint projektet érintő gazdasági és műszaki döntéseket is befolyásolhat. Gyengesége az emberi tényezőtől való jelentős függése, hiszen a felépített modell, információk helyes összerendelése (hibák, hibamódok, okok, funkciók) és az egyes funkciók- és hibamódok érthető megfogalmazása, valamint ezek eredményre vezető kiértékelése teljesen a készítőktől függ. Gondolok itt arra, hogy az FMEA-ban olyan elemzést készítenek, amely mind a későbbi gyártás számára feldolgozható információt tartalmaz, illetve a termék biztonságos használatától eltérő eseteket tárnak fel és értékelnek ki. A kapacitásigényes és sok szakértői szintű tudást igénylő munkát, a módszertanban járatos moderátornak kell összefognia. Számos esetben a moderátor nem ismeri a terméket tervezői mélységében, de a szakértők sem járatosak eléggé mélyen az FMEA modellezésben. Ez nem is várható el a résztvevőktől.

Egy jó elemzéshez célszerű az egyes hibák mélyebb megismerésének érdekében elemezni egy hiba létrejöttének a folyamatát, a létrejöttében kulcsszerepet játszó elemi események kialakulásának logikai megismerését és azok átmenetek valószínűségét felmérni. Az információk rendezésében segítséget nyújthatnak a bemutatott hibafa és hibamód és – hatás elemzési módszerek, hiszen a hibafa elemzés, a fő esemény vizsgálatával bővebb információt szolgáltat a csúcsesemény és az elemi esemény között modellezett gráf szerű logikai kapcsolaton keresztül a hiba létrejöttéről. Az FMEA ezt tovább bővítve, az egész modellezett rendszert vizsgálva mutatja ki a rendszert érő több hiba egyenkénti hatását. Az így kiszámított kockázati szám segít a kockázat sorrendbe állításában.

3 EGYSÉGESÍTETT RENDSZERMODELLEZÉS

Egy összetett és nehezen átlátható kapcsolati rendszerrel rendelkező, intelligens szoftveres vezérlést alkalmazó elektromechanikai termék átfogó modellezése jelentős erőforrásokat emészt fel. Egy-egy modell összehasonlíthatósága és későbbi újrahasználhatósága nem csupán gazdasági kérdés. A modellalkotás első nagy kérdése az absztrakció megfelelő szintjének megválasztása. Egy tapasztalt, átfogó ismeretekkel rendelkező szakértői munkacsoportot igényel, ami költséges tud lenni és sok időt igényel. Azonban kifizetődővé válik ez a befektetés, ha a tervezési szakaszban már ki lehet szűrni jelentős kockázatú, a termék- és emberi élet biztonságát is kockáztató hibákat, tényezőket. Egy hatalmas és komplex modellel szemben olyan alrendszereket, rendszerek-rendszereit és komponenseket kell azonosítani, amelyek elég jól körülhatárolhatók, elkülöníthetők az egyes funkciók hatásvonala és be-kimeneti állapotai egyértelműen nyomon követhetők [63].

A különböző műszaki, mérnöki fejlesztési területek, mint például az elektronikus hardver (hw), szoftver (sw) és mechanika (mech) eltérő tartalmú és célú modelleket alkalmaznak. Az elemezendő termék egészének vizsgálatára a klasszikusan értelmezett „system engineering” azaz „rendszermérnök” szemléletet célszerű alkalmazni, amely e területek egészét vizsgálja magas szinten és nem célja a túlságosan mély, részletekbe menő elemzés. A hangsúly tehát egy átfogó rendszermodell elkészítésén van, ahol a termékkel kapcsolatban kapott vagy megfogalmazódott követelményekre kell építeni és modellezni [44]. A modellezésben két megközelítés alkalmazható, a felülről-lefelé (top-down) vagy a lentről-felfelé (bottom-up) felépítés. Az FMEA-ban a felülről-lefelé megközelítést célszerű alkalmazni. A felső szintet a jármű vezetője által tapasztalható hatásokat, funkciókat célszerű tekinteni, míg az alsó szintnek az alkatrészek közötti együtthatásokat, amelyek a jármű vezetője számára sokszor láthatatlan és nem tapasztalható meg. Mind a két módszer esetén kiemelten kezelendő a nyomonkövethetőség (traceability) elve, azaz a logikai kapcsolatoknak követhetőnek kell lenniük [26].

A rendszer szemléletet alkalmazva az FMEA modellezésére két módszert ismertet Stephenson [78]. Az egyiket funkcionális-, a másikat hardver FMEA-nak nevezi [90]. A funkcionális elemzés esetén az egész rendszerben, alrendszerben végigkeresik az adódó hibák lehetséges eredményeit, kiemelve hogy nem csupán a fő rendszerben, hanem a kapcsolódó, másodlagos rendszerekben is vizsgálnak hibahatásokat. Látható, hogy a

rendszer egészére nézve van jelentős hatása a támogató, kapcsolódó alrendszerek vizsgálatának, amelyek a főrendszerhez kapcsolódva hatással vannak annak állapotára. A hardver FMEA esetében az alkatrészeken van a hangsúly, amelyek felépítik az adott részegységet, illetve az alrendszert. A két vizsgálati módszer együttes alkalmazása is lehetséges és célom is – egy közös rendszer megbízhatósági elemzésben.

3.1 Hibamód és -hatás típusai és az elemzés készítése

A VDA 2006-os kiadása [68] az FMEA-t három nagy csoportba osztja. Az egyik a termék tervezéséhez kapcsolódó rendszer (System) és konstrukciós (Design) FMEA, amely egy rendszer funkcióit, illetve a fizikai alkatrészeket elemzi a követelményekre támaszkodva. A másik csoport a gyártási folyamat (Process) FMEA, amely a gyártásra fókuszál, az abból adódó kockázatokat vizsgálja [68]. Az elemzés elvégzéséhez ismerteti a klasszikus „5 step method" azaz „5 lépés módszerét", azt az öt lépést, amelyet mind a termék mind a gyártási modellezésnél alkalmazva elkészíthető egy FMEA elemzés. Ez az öt lépés a következő [68]:

1. Struktúra analízis (áttekinteni a vizsgált terméket, rendszerstruktúra készítése).
2. Funkció analízis (funkciók hozzárendelése a struktúrához, funkciók logikai összekapcsolása).
3. Hiba analízis (hibák hozzárendelése a funkciókhoz, hibák logikai összekapcsolása).
4. Akció analízis (már meglevő hibákhoz megelőző- vagy detektáló intézkedések definiálása).
5. Optimalizálás (kockázatok csökkentése akciókkal, azok újbóli felülvizsgálata).

Megjegyzem, hogy a VDA 2018-as [88] munkacsoporti tervezetében a munkacsoport bővíteni kívánja ezt az 5 lépést 6 lépésre – egy „scope definition"-t bevezetve, azaz cél meghatározási lépéssel, ami a jelenlegi első lépést, a strukturálási folyamatot megelőzi. Ezzel a projekt minél jobb körülhatároltságát és ütemezhetőségét javítja, véleményem szerint a nehezen értelmezhető kapcsolatok, funkciók, kapcsolódó rendszerek, illetve a külvilág közötti interfészek és határvonalak átláthatóbbá válnak.

Az FMEA készítése számos vállalatnál saját folyamataik által előírt módon történik, összhangban természetesen a jelenleg érvényben levő szabványok és iparági előírások elvárásával. Általános jellemző, hogy az AIAG és a VDA, valamint a minőségirányítási

rendszert előíró szabványokat, előírásokat (SAE J1739) együttesen igyekeznek alkalmazni az autóiparban. Ezen szabványoknak megfelelendően három FMEA típust és ezzel együtt munkalap sablont különböztetnek meg:

1. Rendszer FMEA (System FMEA) – rendszer szemléletű, teljes kiértékelést tartalmazó munkalap.
2. Terv FMEA (Design FMEA) – kézzel fogható termékek tervei, alkatrészek elemzésére szolgál.
3. Folyamat FMEA (Process FMEA) – a gyártás, gyárthatóság elemzésére alkalmazható.

Az egyes típusok között logikai kapcsolat létesíthető, amely az elemzések hatékonyságát növelik. Az általánosan használt kapcsolatot a hatás-funkció-ok (effect-function-cause) tartalmakon keresztül írhatók le, de az alkalmazás és megvalósítás már eléggé egyéni és eltérő lehet.

Az FMEA elemzés elvégzéséhez célszerű a kezdeti lépéseket megkönnyítő áttekintő modell készítése. Ezt javasolja a QS9000 követelményrendszer a szemléltető ábrákkal, diagramokkal. Ezek a kezdeti „brainstorming”-ot támogató lépések segítenek elindulni a rendszert veszélyeztető hibák feltérképezésében, valamint az egyes építő elemek körülhatárolásában és egymásra hatásának megismerésében [18]:

- Blokk diagram (BD), amely a rendszerek fizikai, logikai kapcsolatát szemlélteti,
- Paraméter-diagram (P diagram), amely strukturálisan elemzi a fizikai jellemzőket.

Az elemzést a korai kockázatelemzésen túl további módszerekben is alkalmazzák. Ilyen az FMEA alapelvének alkalmazása, például a tesztelés területén [66], ahol egy szoftver rendszerben a definiált hibákat végig vezetik az egyes modulokon, vizsgálva annak hatását, illetve a függőségeket a hibaörökítő képességét. Ezáltal az objektumok sérülékenysége és az egyes szoftveres interfészek hibakezelő képessége kerül megismerésre.

Egyre elterjedtebb a már elkészült analízisből kinyert adatok feldolgozása a fejlesztési idő optimalizálására vagy éppen egy diagnosztikai funkció kidolgozására [74]. Egy újabb területet ölel fel a kockázat kiértékelés finomítása, fuzzy elmélet alkalmazása [62] és a modell alapú FMEA készítés [80].

3.2 Szoftver elemzése FMEA-val

Az egyik legkiemelkedőbb különbsége a szoftver komponensnek, hogy az elektronikus hardver- és mechanikai komponensekre jellemző „kádgörbe”, azaz az elkopás, a gyártási hibák, a termékkihordás nem jellemző, sokkal inkább logikai vagy tervezési hiba fordulhat elő [34]. Az összetett, beágyazott szoftverrendszerek elemzésénél időnként nehezen határolható körül a kielemezendő komponens, nem könnyű eldönteni, hogy a szoftveren belül mit tekintsünk funkciónak vagy mely az a mélység az elemzésben, ameddig van értelme elmenni. Az egyes szoftvermodulok sokszor több ponton kapcsolódnak egymással, aktuális állapotukat valamely preferencia alapján módosítják a külvilág számára érzékelhető funkciók meghívása dinamikusan történik, amely függhet a futtató hardveres eszköz szenzorjait érő hatásoktól is. Összefoglalva, alkalmanként nehéz pontosan leírni, hogy mikor mi hívódik meg, átlátni egy adott funkciónak vagy az általa végzett számításnak hatását egy másik modulra, illetve az egész rendszerre nézve. Természetesen léteznek modellezési eszközök, mint például az Unified Modelling Language (UML) vagy folyamatábrák, de ezek általában egy pillanatkép készítésére vagy egy-egy elkülönült modul ideális működési állapotnak leírására szolgálnak [91]. Az esemény kombinációk hatásaira azonban az uszodasávos (swim lane) leírás is csak részben nyújt megoldást, mert a párhuzamosság egy bonyolultabb algoritmus esetén nehezen szemléltethető egyértelműen.

A fizikai eszközön futtatott szoftver szervesen kötődik az azt futtató elektronikus eszközhöz, amelyet működtet. Megbízhatósági vizsgálatok esetén célszerű ezért a közismert „jelfolyam követés” elvét alkalmazni, amelyben az elektronikus eszköz kézzel fogható portjától indul az elemzés egészen az adott szoftvermodulig. Darryl cikkében kiemeli, hogy a szoftverek elemzésekor itt is törekedni kell az egyszeres hibák elemzésére, illetve a hiba továbbterjedési lehetőségére. Kiemeli, hogy a szoftver FMEA-ban általában előforduló kihívások a következők [40]:

- A szoftver nem állít elő hibákat normál működés és használat közben, a hiba események tipikusan nem határozható meg előre.
- A hibák (failure) explicit eredményei a meghibásodásnak (defect), amely belépül a szoftverkódba – ismeretlenül, implicit módon.
- A hibamódok általában ismeretlenek és függnek az adott műszaki megoldás dinamikus viselkedésétől.

Haapanen [31] tanulmányában a szoftver komponenseket „system software” (rendszer szoftver) és „application software” (alkalmazási szoftver) csoportokra osztva két szinten vizsgálja. A „system software”-t egyszerű operációs rendszer esetén tovább bonthatónak tekinti „system kernel”-re és „system services”-re. Ez a két utóbbi az operációs rendszer esetében lényegében a rendszer működtetését (rendszerbetöltés, inicializálás, önteszt, stb.) és a különböző célú adatkezelést és műveletek elvégzését foglalja magában.

Haapanen 2002-es közleményére az utóbbi években hivatkozók hozzáférhető forrásokat áttekintve megállapítható, hogy a legtöbben (körülbelül 70%) az FMEA általános használatának módszertani használatával kapcsolatosan idézik. Ilyen például Martinis és szerzőtársai, akik az FMEA első alkalmazására hivatkoznak (Amerikai Hadsereg egy szabványban rögzíti), míg Vrieze az FMEA hibaelemző tulajdonságát emeli ki a cikkében. [49] [59]. A további cikkekben csupán a szoftver tartalom elemzésére utalnak, miszerint azt nehéz vagy szinte lehetetlen FMEA-ban elemezni, mert elsősorban hardverre alkalmazzák. [69]. A Rising és Levenson szerzők szerint a szabvány is állítja, hogy maga az elemzés nem kivitelezhető szoftveren, vagy legalábbis minimálisan valósítható meg elvileg, de nem talált evidenciát arra, hogy ezt bizonyítsa. Erre hivatkozták meg az FMEA IEC által 2016-ban kiadott leírást. [5].

Végül, egy cikk csupán megemlíti a szoftver komponensek eltérő szempontú elemzését Haapanen-re hivatkozva, de nem vezeti tovább ezt a gondolatmenetet [13]

Az egységes modellezésben elkerülhetetlennek tartom a szoftver elemzését, ezért dolgoztam ki három, jól elkülöníthető csoportot, amelyek egymásra épülési logikájuk miatt szinteknek tekintek. Kettő szoftver szint hasonló elvű, mint amit Haapanen megfogalmazott, azonban egyel kiegészítettem. Lentről felfelé haladva az alábbi [41]:

1. Platform szint, az elektronikus hardverhez kötődő, működtetéshez szükséges komponensek. (Haapanen modelljében a „system kernel” vagy éppen „system software” szintet foglalja magában.)

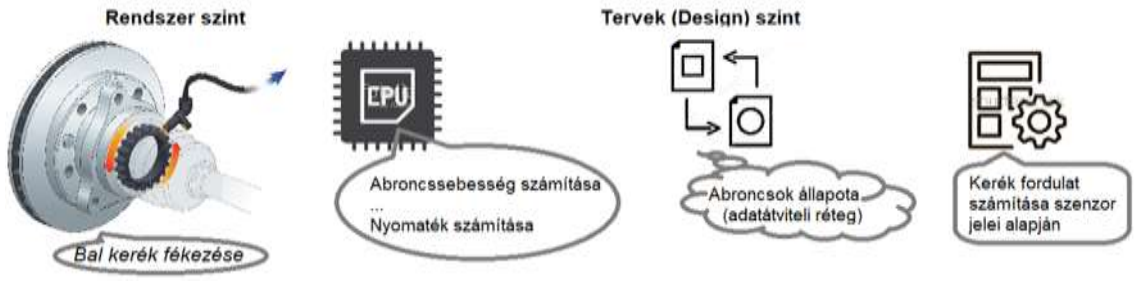
2. Adatátviteli szint, a kommunikációs tömbök és változók az egyes szoftver modulok között. Ez a réteg alapja lehet az interfészek definiálásának, a cél a definiált paraméter átadásában megjelenő változók hibás értékének vizsgálata, hatásának felmérése a rendszerre. Ilyen lehet a DML (Data Management Layer), vagy egy hálózati üzenet is.

3. Rendszer szint, a magas szintű funkciók, számítások elvégzését végző komponensek. (Haapanen modelljében az „application software”, illetve a „system services” réteget foglalja magában; a hardvertől független szolgáltatások.)

Az adatcsere és az interfész vizsgálatát elkülönítetten kezelem, mert az adatátvitel meghibásodásának kockázatát nem szabad elhanyagolni manapság, hiszen a biztonság (security) egyik támadási pontja a kommunikációs pontatlanságok kihasználása. Egy funkcionális biztonsági szabványból (ISO 26262) kiinduló, de azt kiber biztonsági vizsgálattal kibővítő publikáció is felhívja erre a figyelmet. A szerzők definiálnak négy csoportot (kommunikációból kiindulva): fizikai réteg, adattovábbítás és megjelenítés. A csoportokhoz attribútumokat rendeltek az autóipari szabványok előírásaira támaszkodva (ISO 26262, SAE J3061, ASPICE), amely paraméterek (például: fizikai minimum-maximum érték, működési üzemmódok, időzítések, szoftver által megjelenített minimális-maximális érték, stb.). A szoftver szemszögből elemezett adatok felhasználhatóak lehetséges hiba gyökér okokként, amelyeket szintén be lehetne építeni az FMEA-ba is. A szerzők ugyan egyéni analizálást írnak le publikációjukban, de véleményem szerint ez könnyen felhasználható az FMEA-ba is. [47] Azonban nem szabad feltételezni, hogy a megoldás helyettesítheti a teljes biztonsági (security) felmérést, mert a TARA[5] nem csupán a termékre fókuszál, hanem a fejlesztés körülményeire, gyártásra, stb.. A biztonsági (safety) és (security) együttes elemzésére végzett elemzést Plósz vasúti járműrendszereket elemezve a Microsoft Threat Modeling eszközét és az FMEA eredményeit felhasználva készítettek elemzést. Érdekesség, hogy újra használható hiba- és kiber támadástípus katalógust állítottak elő az elemzés során. [13].

A 3.1 ábrán ezeknek a szinteknek egy alkalmazása látható a keréksebességmérő szenzor sebességmeghatározásán keresztül. Itt a magas, rendszer szintű funkciót egy bal kerék fékezése jelenti, amelyhez kapcsolódik az abroncs állapotát meghatározó, járműre szabott alrendszer. A platform szinten található a vezérlő mikrokontrollert működtető szoftvercsomag, amelynek része a kerékfordulatot figyelő szenzor jeleinek illesztése és feldolgozása mérnöki mértékegységgé (például fordulat/percre). Az abroncs állapotát meghatározó rendszer és a szenzor jeleit feldolgozó komponensek között egy adatátviteli réteg juttatja el az aktuális mért értékeket.

[5] Threat Assessment and Remediation Analysis: egy elemzés, amelyben felmérik és priorizálják a lehetséges kibertérből jövő támadásokat. Az azonosítást követően akciókat dolgoznak ki, amelyekkel csökkenteni tudják a rendszer sérülékenységét. [93]



3.1. ábra Példa a szoftverkomponensek közötti

A biztonságkritikus rendszerekben szükséges meggyőződni egy adott periférián érkező adatok hitelességéről, vagy éppen megfelelő működéséről. Ezeket rendszerint vagy elfogadhatósági vizsgálattal (Plausibility Check) vagy monitorozási rutin előírásával végzik el. Ezen rutinok bevezetése rendszerint biztonsági elemzések eredménye is lehet, ezért célszerű azok helyes működéséről meggyőződni. Azonban nem kis kihívást jelent az értelmezésük, mert elvileg a hardvertől függetlenül működnek ezek a rutinok. Így egy rutin meghibásodását logikailag nem tudjuk hová kötni, ugyanakkor nincsen más kapcsolódó modul az adott műveletvégző hardver elemeit leszámítva, ami a helyes szoftver üzemszerű futtatását befolyásolná. Tehát, a hardverhez köthető monitorozó rutinokat célszerű elemezni, szemben a szoftver alapú, a szoftvert ellenőrző rutint, amit nem célszerű mélyebben elemezni, mivel véget nem érő elemzésekbe lehet belekerülni, ha egy adott szoftver meghibásodása azonos szinten levő elemek egymásra gyakorolt meghibásodását analizáljuk. Lehetséges ugyan a fejlesztői környezet, a fordító hibázási lehetőségének elemzése, de ezeket célszerű folyamatokkal védeni, biztosítani. Ilyen lehet például a beállításokat nem szabad módosítani egy adott szintű validációt követően a termék fejlesztési életciklus adott érettségi szintjét követően. Van erre ugyan esély, hogy a fordító vagy a fejlesztői környezet hibájából rosszul hajtódik végre a forráskód, például a fordítóprogram (compiler) gyártója által kiadott hibalista információval nyilvánvalóan követhető és kezelhető.

A szoftver elemzését véleményem szerint célszerű rendszer (system) szinten kezdeni, szemben Johanyák véleményével, aki a konstrukciós (Design) FMEA-ban kívánja kidolgozni. A szoftvert három módon javasolja elemezni [38]:

1. modul alapú megközelítés, a szoftvert modulokra bontja és megkeresi ezek hibalehetőségét;
2. feladatközpontú megközelítés: a szoftver funkciói szerint haladva történik a vizsgálat;

3. helyzet alapú megközelítés: lehetséges működésből kiindulva megkeresi a hibát előidéző rendszerelemeket.

Egy gépjárműipari, biztonságkritikus beágyazott szoftver elemzésében tapasztalatom szerint az a leghatékonyabb, ha a modul alapú megközelítést alkalmazzuk. Gyakori tapasztalat, hogy a szoftverfejlesztők nem fordítanak kellő hangsúlyt a moduljaik be- és kimenetének megfelelő definiálására vagy éppen a bejövő adatok helyességének ellenőrzésére. Gondolok itt különösen arra, amikor értékpárokkal vagy kombinációkkal dolgoznak, esetleg nem fordítanak kellő figyelmet az érkező adat lehetséges nagyságára és kétszer akkora biten érkező adatból csak fele annyi bitmezőt fogadnak. Ez természetesen szoftver tervezési, architektúrát érintő kérdés, de lehet jól definiált, ha a kivitelezésbe hiba csúszik. Ugyanakkor a megbízhatóságot javítja, ha ezt is figyelembe vesszük. Nem is beszélve arról, hogy újkeletű kérdés a biztonság (secuirty) kérdése, amely pedig az ilyen interfészekre fókuszál. Ezért tartottam fontosnak, hogy a szoftver FMEA készítésénél ne csupán a rendszer adatainak felvételére fókuszáljunk, hanem Darryl közleményében megfogalmazottakhoz hasonlóan az elemzést végző csapatot előzetes információval készítsük fel a megbeszélésre. Ennek megfelelően az FMEA moderátor mellett a többi résztvevő számára is átláthatóvá válik az elemzendő modul működése [40].

3.3 Elektronikus és mechanikai hardver elemzése FMEA-val

Mind a két esetben, hardver és mechanika leginkább a konstruktív (Design) FMEA munkalapot alkalmazzák. A fizikai komponensekre (hardver, mechanika) épülő elemzés lényegében a rendszert felépítő alkatrészek, komponensek meghibásodását és megbízhatóságát vizsgálja. Az elemzés készítésekor jellemzően az alkatrészeket tartalmazó listára a Bill of Material (BOM)-ra támaszkodnak. A szoftveres FMEA elemzéshez képest erről a témakörről sajnos kevesebb irodalom áll rendelkezésre, feltehetően az egyértelmű és tradicionális elemzés alkalmazása miatt, mivel az FMEA-t is eredetileg erre a célra alkották meg. Az elemzésben felhasználnak végeselemes, multi-fizikai szimulációkat és mechanikai, fizikai vizsgálatok eredményeit a pontosabb hibamódok előfordulási valószínűségének meghatározására, feltárására. Elmondható, hogy az elektronikus eszközök és mechanikai komponensek FMEA-ja többnyire hasonló elvek szerint csoportosítható és rendezhető, azonban az elemzésük tartalma (egy FMEA lap tartalma) a gépészeti- illetve félvezetőkre jellemző elektronikus tartalom miatt eltérő [41].

Az elektronikus hardver elemzésének elterjedt módszere az adott komponenst üzemképtelenné tevő meghibásodások vizsgálata. Itt tipikus hibákat vesznek fel: rövidzárlat vagy szakadás, illetve driftelés[6]. A funkcionális biztonság megjelenésével az Failure Modes, Effects and Diagnostic Analysis (FMEDA) elemzés kerül előtérbe, amely az FMEA-ból fejlődött ki [12]. A hardver elemeken nem alkalmaznak speciális karakterisztikákat, ami a gyártásban szükséges Statistical Process Control (SPC) biztosításához szükséges [89], mivel az alkatrészeket a gyártás során alapesetben is többször átvizsgálják, például pozicionálás megfelelését a beültetésnél (különösen a Surface-Mount Devide – SMD[7] esetén), illetve áramköri méréseket végeznek el az áramkör élesztésekor a gyártósori teszt részeként.

Ezzel szemben a mechanikai komponenseket olykor speciális, Critical Characteristic (CC) és Special Characteristic (SC) karakterisztikákkal látják el az adott vállalat minőségirányítási rendszerében definiált súlyossági (S) és előfordulási (O) értékek alapján. [55] Célja, hogy egy-egy speciális tulajdonság (például átmérő, anyaghasználat, stb.) ami a gyártás számára fontos jelentőséggel bír a termék minőségének befolyásolása szempontjából külön ellenőrzésre kerüljön egy mérhető, illetve biztosítható mennyiség vagy tulajdonság alapján, az SPC szabályozással. Az alkatrészek vizsgálatakor célszerű azokat valamilyen szempont szerinti csoportba sorolni, hogy követhetőbbé váljon a rendszer felépítésben. Az elemzések jellemzően egy-egy alkatrész funkciójára vagy geometriai, műszaki paraméterére fókuszálnak. Ezt a jól ismert tulajdonságot kihasználva végzett kísérletet Nigel Hughes csapata is, megállapítva hogy az FMEA mechanikai elemzéseinél fontos a geometriai és a kapcsolódó gépészeti információk. Mindezeket egy CAD/CAM rendszer vezérléséhez szükséges automatizált modell generáláshoz használták fel sikeresen, egyszerűbb alkatrészek esetén [35].

3.4 Következtetések, ajánlások

A fejezetben bemutattam az FMEA-t alkalmazó mérnöki diszciplínák elemzésének főbb jellemzőit. Az egyes diszciplína igénye eltérő fókuszú és struktúrájú, ezért fontosnak látom megoldani az egységes, sablon szerű elemzés bevezetését, valamint az egyes formanyomtatványok csoportosításának optimalizálását, hogy a gyártás számára is használható információ állhasson rendelkezésre a fejlesztést követő évtizedek múlva is.

[6] drift, másnéven „sodródási áram”: A félvezetőben külső vagy belső villamos erőtér hatására kialakuló határozott irányú töltés áramlás. [50]
[7] SMD: az áramköri NYÁK felületére ragasztott, majd forrasztott aktív és passzív áramköri alkatrészek.

A termékek fejlesztési életciklusára (development lifecycle) jellemző elvárások miatt egyre jobban megfogalmazódik az újra felhasználhatóság és változások kezelésének jelentősége a vállalatok számára. Ezeket jól követhető módon kell dokumentálni, mivel mind az auditokon mind egy esetleges későbbi termékfelelősségi vizsgálaton hatóságilag is vizsgált téma. Szintén vizsgálatra kerül egy homologizáció[8] esetén, ahol nem csupán a meglétét, hanem műszaki tartalmát is áttekinti az engedélyező hatóság.

A fejezetben bemutattam egy új, általam kidolgozott FMEA modellezést támogató szoftver tagolási modellt, amely a biztonságkritikus autóipari szoftverrendszerek FMEA célú elemzéséhez használható fel. A disszertáció írása közben derült ki számomra is, hogy az ismertetett módszerem lényegében Haapanen 2002-es publikációjának [31] egy továbbfejlesztése a szoftver FMEA-beli modellezésében. A már ismertetett három logikai szint az egyes modulok csoportosításával átláthatóbbá és sematikusabbá teszik az FMEA-t. A biztonság (security) egyik támadási pontjának számít a kommunikáció (paraméter átadás, értelmezés) kérdése. A szoftver FMEA-ban egy külön logikai szintként kerül modellezésre, ez által jobban kirajzolódhat egy-egy adatcsomag hibája és annak a rendszer egészére gyakorolt hatása.

Bemutattam továbbá a hardver és mechanika területek egy új modellezését, amely segítségével a hardver és mechanikai alkatrészeket logikai csoportokba soroltam. A speciális karakterisztikákat (SC, CC) az általános gyakorlattól eltérően logikai csoport szintjén definiálom az adott tulajdonsághoz rendelve, hogy a későbbi változtatásoknál követhető legyen a definiálás indoka. Az új szemléletmódban a tervezés kiértékelése és nem a megoldás szintjének vizsgálata áll középpontban egy előre meghatározott sablon segítségével, mivel a tervezési szempontok figyelembevétele kerül vizsgálatra.

Rámutattam, hogy az interfészek vizsgálata egyre fontosabbá válik a sebezhetőségi lehetőségek miatt, amelyet kielemezve olyan információhoz juthatunk, amely más megkívánt elemzés számára is szolgáltathat hasznos információt.

[8] Homologizáció: egy hatósági eljárás, amely eredménye egy okirat arról, hogy a vizsgált termék teljesíti az adott régióra előírt biztonsági és műszaki előírásokat. [24]

4 KOCKÁZATI ÉRZÉKENYSÉGVIZSGÁLAT

Mindennapjainkban gyakran nézünk szembe kockázatokkal, amelyet egy kiváltó okot követő leginkább negatív vagy olykor pozitív irányú hatással jellemezhetünk. A kiváltó ok bekövetkezése általában egy valószínűségi értékkel becsülhető, lényegében a fejlesztések, projektek velejárója. Egy-egy felismert, veszélyt rejtő kockázati tényező megfelelő szintű kezelése minden szakember feladata munkakörtől és döntéshozatali feladatkörtől függetlenül. A termékfelelősségi jog hatásköre magába foglalja, hogy a fejlesztés tisztában legyen az általuk fejlesztett termék használatából adódó kockázatokkal és rangsorolja, illetve kezelje azokat a társadalmi elvárásoknak megfelelően. Ehhez kockázatelemzést szükséges elvégezni, amelyet lehetséges a már említett kvalitatív (minőségi skálán kiértékelő), illetve kvantitatív (mennyiségi vizsgálat vagy számszerűsített valószínűségi elemzés) módon elvégezni [14]. A mérnöki tervezés szempontjából kézzel foghatóbb és könnyebben kezelhetőbb a számszerűsíthető kvalitatív módszer, míg a kvalitatív módszerre általánosan alkalmazható a már ismertetett FMEA módszertan. A kvantitatív módszer egyik halmaza a valószínűségi elemzés, amely a valószínűségi eloszlások alkalmazásával számszerűsiti a vizsgált kockázatokat. Egyik lehetséges kiszámítási módja a valószínűség és hatás szorzatából adódik [65]. Az érzékenységi vizsgálattal egy rendszer valamely paraméterének megváltoztatásával ismerhető meg a rendszer egészének stabilitása, biztonsága és robusztussága a változás hatásának ellenében. Általában a bemeneti paramétereket vizsgálva kerül elemzésre a rendszer által adott válasz [63].

A NASA-GB-8719:13-2004 [56] szerint a kockázat kiértékelését két módon is el lehet végezni: követelmény menedzsmenten keresztül a kritikusnak azonosított elemek követhetőségét fenntartani és megjelölni, valamint elhatárolni a nem kritikus eseményektől, megelőzve a „biztonsági funkciók beszennyeződését”. Azonban nem világos, hogy miként azonosít egy elemet kritikusnak, illetve hogyan szándékozik csökkenteni a nem kívánt esemény bekövetkezését. Egy rendszerbeli kockázat mértékének megismerésére az FMEA-t, míg egy adott esemény vagy elem bekövetkezésének pontosabb megismerését a hibafa módszerrel legcélszerűbb elvégezni az iparág minőségirányítási gyakorlatával összhangban.

4.1 Hibát kiváltó elemi tényezők azonosítása és vizsgálata

Egy magas szintű biztonsági előírásoknak megfelelő rendszerben szükséges az egyes hibaokok kialakulásának, felépülésének és kapcsolatrendszerének megismerése. A hibaokok

azonosításában általában a korábbi fejlesztések tanulságai (lessons learned), első közúti járműtesztek terepi (field) tapasztalatai és a vásárlói tesztek validációs eredményei, illetve maga az FMEA ad kiindulási alapot. Azonban a mélyebb hibaok vizsgálatához már a hibafa (FTA) módszert érdemes alkalmazni. Az alapfunkciók esetén azonban nem szabad itt megállni, szükséges a hibaokot kiváltó elemi hibák közül a legkritikusabbat megtalálni. Ennek ismeretében a legkritikusabbnak számító elemi hiba ellen további intézkedéssel még robusztusabbá tehető a tervezett rendszer. Lehetséges az elemi hibák halmazából vágatokat (cut set) vagy útvonalakat (path set) kinyerni, de az idő rövidsége miatt előnyösebb lenne egy jól algoritmizálható, objektív formában rendelkezésre álló módszert alkalmazni. Erre alkalmas egy mátrixalgebrai módszer, amely ’Linear Fault Tree Sensitivity Model’ (LFTSM) (Lineáris Hibafa Érzékenységi Modell) módszerként került publikálásra [76] [75]. Alkalmazásával meghatározható egy rendszer adott paraméterekkel szembeni érzékenysége, ami jelen esetben a hibafát kielemezve megmutatja, hogy az elemi hibák közül a rendszerre nézve melyik a legérzékenyebb. Erre a módszerre építve végeztem el egy vizsgálatot, a beágyazott szoftvereket futtató rendszerek szisztematikus fejlesztési hibáit elemezve. Mint köztudott, a szoftver meghibásodási lehetősége nem elhanyagolható mértékben függ a fejlesztők által betartandó szabályoktól és munkacsomagoktól, amelyeket fejlesztési folyamatokkal és intézkedésekkel igyekeznek szabályozni. Egy vállalatnak jó esetben lételeme a folyamatos fejlődés iránti igény, amelyhez egy-egy életszerű felhasználásból eredő visszacsatolásra támaszkodhat. Ilyen lehet egy folyamatból eredő hiányosság feltárása, ami megkönnyítheti a minőségirányítás folyamatfejlesztési feladatát. Erre alkalmaztam Pokorádi [64] módszerét, de egy műszaki probléma helyett egy FMEA elemzésből szolgáltattam bemeneti adatokat.

Első lépésként a gyökérok (root cause) kialakulásának feltérképezésére hibafát készítettem. Az elemi és köztes hibák hatása eltérő kockázatot jelent a csúcsesemény bekövetkezésére nézve. Az egyes elemi eseményekhez tartozó hibákat az elemzett termék FMEA-jából olvasom ki. A fejlesztési hibák előfordulását pedig az adott hibához rendelt előfordulási (occurrence) pontszámot (1-10) a SAE J-1739 [71] katalógusban megadott gyakorisági érték alapján számítom. A bekövetkezési valószínűség (P_i) értéke, az elemi hibákat hiba típusokba csoportosítva, azokhoz rendelt valószínűségi érték adja. Ezt mutatja a 4.1 táblázat.

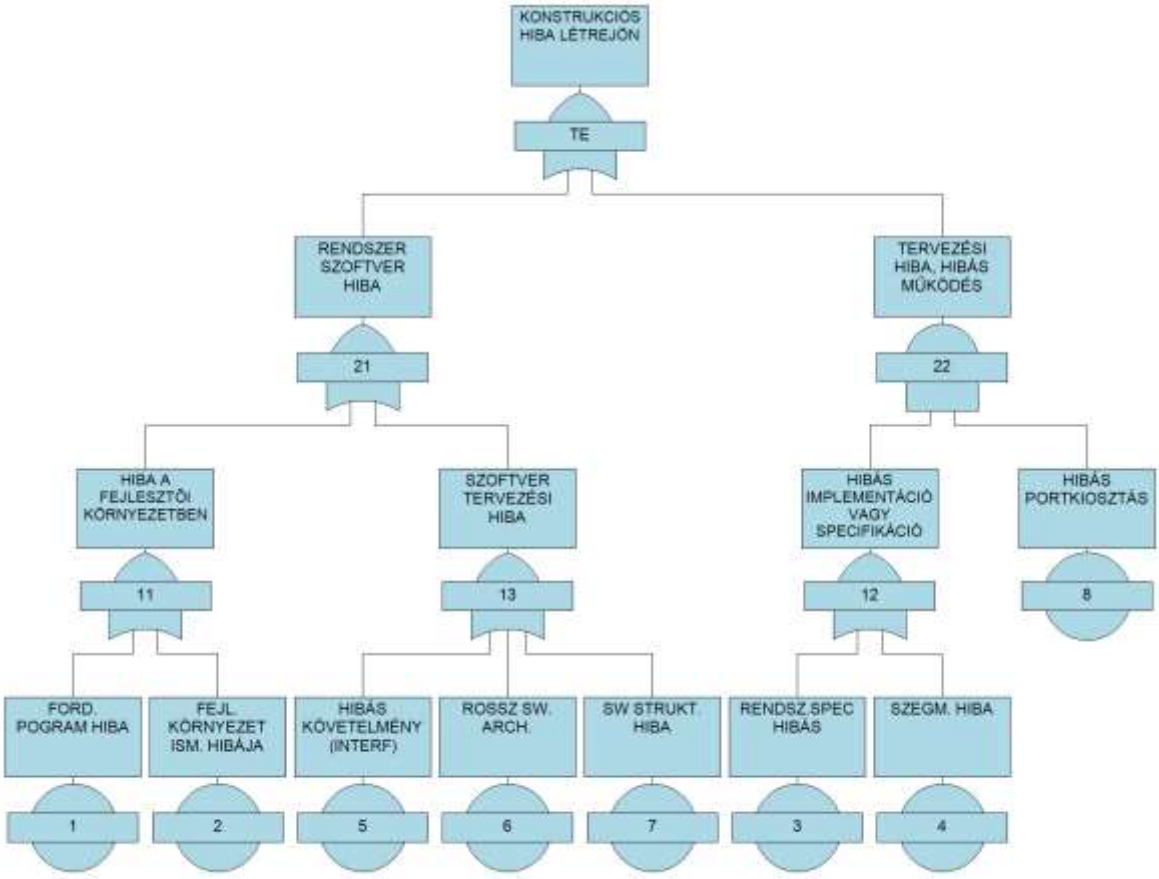
.

i	Hiba típusa	Valószínűség P_i
1	fordítóprogram (compiler) hibája	0,0005
2	errata check (fordítókörnyezet ismert hibáinak figyelembevétele)	0,002
3	rendszer specifikáció követelményeit hibásan implementálták	0,01
4	szegmentációs hiba	0,005
5	hibásan implementált követelmények (interfész szempontjából)	0,01
6	rossz szoftver architektúra alkalmazása	0,005
7	nem megfelelő strukturáltságú szoftver	0,005
8	a hardver felépítés szintű hibás port kiosztás	0,0005

4.1. táblázat Elemi események és előfordulási értékei

A csúcseseményhez az elemi hibák kombinációin keresztül lehet eljutni. A vizsgálat tárgya megtalálni az elemi eseményeket vagy azok kombinációit, amelyektől a rendszer a legsérülékenyebb és amely veszélyezteti a rendszer egészének stabil működését.

A 4.1 táblázatban felsorolt elemi események a hibafa kiinduló pontjai, a hozzájuk tartozó valószínűségi értékek a következő szintre lépés bekövetkezésének esélyét jelölik. Azonban a csúcsesemény eléréséhez az elemi események logikai kombinációiból is adódhatnak köztes hiba állapotok. Ezért ezek a köztes szintek adott állapotai közötti valószínűségi értékeik az adott eseményhez kapcsolódó, egy szinttel lentebbi eseményeinek logikai kombinációjával kerül kiszámításra. A felírt hibafán, alulról felfelé haladva látható a sorszámozás, mert az elemi eseményekből indulva kerül felépítésre a hibafa, amely a 4.1 ábrán látható [76].



4.1. ábra Vizsgálati hibafa a konstrukciós hiba létrejöttére

A 4.1 ábrán az alsó szinten látható számok 1-7 a 4.1 táblázatban látható elemi hibák *i* értékét jelölik. A P_i valószínűségi értékek a (4.1) – (4.6) egyenletekben kerültek felhasználásra rendre P_1 ... P_7 értékekben. Az elemi- és csúcsesemény közötti közbenső, nem elemi események valószínűségi értékeit „ÉS”, illetve „VAGY” logikai kapcsolatokkal határozhatók meg a (4.8) és a (4.9) egyenlet felhasználásával az alábbi módon:

$$P_{TE} = 1 - ((1 - P_{21})(1 - P_{22})) \tag{4.1}$$

$$P_{21} = 1 - ((1 - P_{11})(1 - P_{13})) \tag{4.2}$$

$$P_{22} = P_{12}P_8 \tag{4.3}$$

$$P_{11} = 1 - ((1 - P_1)(1 - P_2)) \tag{4.4}$$

$$P_{12} = 1 - ((1 - P_3)(1 - P_4)) \tag{4.5}$$

$$P_{13} = 1 - ((1 - P_5)(1 - P_6)(1 - P_7)) \tag{4.6}$$

Mátrix algebrai módszer alkalmazásával az elemi eseményeket felírhatóvá teszi érzékenységi függvényekként, általános lineáris egyenletek formájában. [64] Ezek alapján felhírható az általános egyenlet (4.7), ahol δ a változók relatív eltéréseit jelzik.

$$\delta y = K_{y;x_1}\delta x_{y;x_2} + \ \ldots + \ K_{y;x_k}\delta x_k \quad , \tag{4.7}$$

Az érzékenységi együtthatók a közbenső események logikai kapcsolatának kifejezésére, általános formában az alábbi módon írhatók fel:

- „ÉS" kapu:

$$\mathrm{K_i} = 1 \quad \forall\, \mathrm{i}\epsilon\{1,2,\ldots,\mathrm{k}\} \quad ; \tag{4.8}$$

- „VAGY" kapu:

$$K_j = \frac{P_j}{P} \prod_{\substack{i=1 \\ i\neq j}}^{k}(1-P_i) \quad \forall\, j\epsilon\{1,2,\ldots,k\} \quad . \tag{4.9}$$

A korábban felírt (4.1) – (4.6) egyenleteket kibővítve a logikai csomópontok kapujának (4.8) – (4.9) figyelembevételével az alábbi paraméterek írhatók fel:

$$\delta P_{TE} = \ K_{21}\delta\, P_{21} + \ \ K_{22}\delta\, P_{22} \tag{4.10}$$

$$K_{21} = (1-P_{22})\frac{P_{21}}{P_{TE}} = 0{,}9997 \tag{4.11}$$

$$K_{22} = (1-P_{21})\frac{P_{22}}{P_{TE}} = 0{,}00003254 \tag{4.12}$$

$$\delta P_{21} = \ K_{11}\delta\, P_{11} + \ \ K_{13}\delta\, P_{13} \tag{4.13}$$

$$K_{11} = (1-P_{13})\frac{P_{11}}{P_{21}} = 0{,}1091 \tag{4.14}$$

$$K_{13} = (1-P_{11})\frac{P_{13}}{P_{21}} = 0{,}8887 \tag{4.15}$$

$$\delta P_{22} = \ K_{12}\delta\, P_{12} + \ \ K_8\delta\, P_8 \tag{4.16}$$

$$K_{12} = 1, \quad K_8 = 1 \tag{4.17}$$

$$\delta P_{11} = \ K_1\delta\, P_1 + \ \ K_2\delta\, P_2 \tag{4.18}$$

$$K_1 = (1-P_2)\frac{P_1}{P_{11}} = 0{,}1997 \tag{4.19}$$

$$K_2 = (1-P_1)\frac{P_2}{P_{11}} = 0{,}7999 \tag{4.20}$$

$$\delta P_{12} = \ K_3\delta\, P_3 + \ \ K_4\delta\, P_4 \tag{4.21}$$

$$K_3 = (1 - P_4)\frac{P_3}{P_{22}} = 0{,}001331 \tag{4.22}$$

$$K_4 = (1 - P_3)\frac{P_4}{P_{22}} = 662{,}2074 \tag{4.23}$$

$$\delta P_{13} = K_5 \delta P_5 + K_6 \delta P_6 + K_7 \delta P_7, \tag{4.24}$$

$$K_5 = (1 - P_6)(1 - P_7)\frac{P_5}{P_{13}} = 0{,}495 \tag{4.25}$$

$$K_6 = (1 - P_5)(1 - P_7)\frac{P_6}{P_{13}} = 0{,}2463 \tag{4.26}$$

$$K_7 = (1 - P_5)(1 - P_6)\frac{P_7}{P_{13}} = 0{,}2463 \tag{4.27}$$

A (4.10) – (4.27) egyenletekben felírt köztes események bekövetkezési valószínűségeit két vektorba kell rendezni. Külön kell választani az elemi (***x***) és a nem elemi (***y***) eseményeket.

$$\mathbf{y}^T = [P_{TE}; P_{21}; P_{22}; P_{11}; P_{12}; P_{13};] \tag{4.28}$$

$$\mathbf{x}^T = [P_1; P_2; P_3; P_4; P_5; P_6; P_7; P_8] \tag{4.29}$$

A vektorok felírását követően a bekövetkezési valószínűségek relatív változásainak együtthatói mátrixban kerülnek meghatározásra:

$$\mathbf{A} = \begin{bmatrix} 1 & -K_{21} & -K_{22} & 0 & 0 & 0 \\ 0 & 1 & 0 & -K_{11} & 0 & -K_{13} \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \ldots$$

$$\ldots = \begin{bmatrix} 1 & -0{,}9997 & -0{,}00003254 & 0 & 0 & 0 \\ 0 & 1 & 0 & -0{,}1091 & 0 & -0{,}8887 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.30}$$

$$\mathbf{B} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ K_1 & K_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & K_3 & K_4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & K_5 & K_6 & K_7 & 0 \end{bmatrix} = \ldots$$

$$\ldots = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0{,}1997 & 0{,}7999 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0{,}001331 & 662{,}2074 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0{,}495 & 0{,}2463 & 0{,}2463 & 0 \end{bmatrix} \tag{4.31}$$

Az események bekövetkezési valószínűgégei és relatív változásai közötti kapcsolat a (4.32)-es egyenlet szerinti mátrix alakban adható meg.

$$\mathbf{A}\delta\mathbf{y} = \mathbf{B}\delta\mathbf{x} \ , \tag{4.32}$$

Ezt átrendezve kapjuk meg a relatív érzékenységi mátrixot, a (4.33)-as összefüggés alapján.

$$\mathbf{D} = \mathbf{A}^{-1}\mathbf{B} \ , \tag{4.33}$$

A **D** mátrix a (4.33) egyenlet *i*-edik sorának *j*-edik eleme azt mutatja meg, hogy az *i*-edik nem elemi esemény bekövetkezési valószínűségének relatív változását milyen mértékben befolyásolja a *j*-edik elemi esemény bekövetkezési valószínűségének relatív változása. A fenti vizsgálattal kapott viszonylagos érzékenységi mátrix:

$$\mathbf{D} = \begin{bmatrix} 0{,}0218 & 0{,}0872 & 0{,}4331 & 0{,}2155 & 0{,}4398 & 0{,}2188 & 0{,}2188 & 0{,}0003254 \\ 0{,}0218 & 0{,}873 & 0 & 0 & 0{,}4399 & 0{,}2189 & 0{,}2189 & 0 \\ 0 & 0 & 0{,}001331 & 0{,}6621 & 0 & 0 & 0 & 1 \\ 0{,}19968 & 0{,}79992 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0{,}001331 & 0{,}6621 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0{,}4950 & 0{,}2463 & 0{,}2463 & 0 \end{bmatrix} \tag{4.34}$$

A mátrix első sorát kiolvasva számítható ki a fő esemény bekövetkezési valószínűségének az elemi események bekövetkezési valószínűségeivel szembeni

érzékenységi együtthatói. A **D** mátrixnak (4.34 egyenlet) ez a sora relatív érzékenységi sorvektorként kezelendő és $\mathbf{d}^T$ -vel jelölve az alábbi sor írható fel:

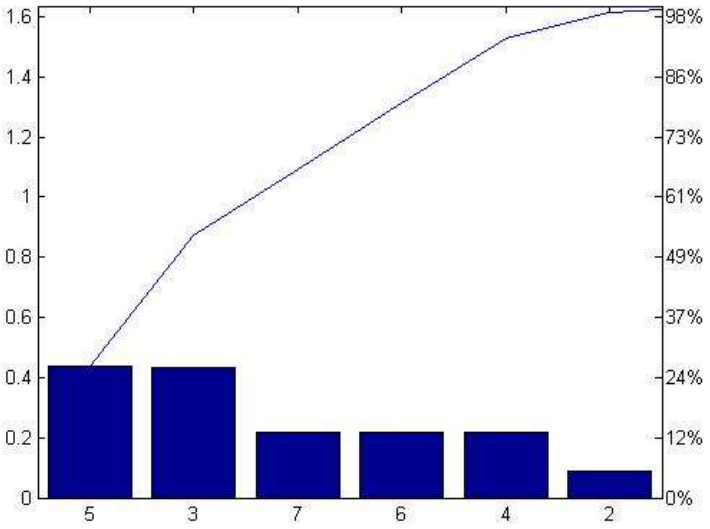
$$\mathbf{d}^T = [0{,}0218; 0{,}0872; 0{,}4331; 0{,}2155; 0{,}4398; 0{,}2188; 0{,}2188; 0{,}0003254] \quad (4.35)$$

A relatív érzékenységvektor kiértékelésére Pareto elemzés alkalmazható, amelynek segítségével kiemelhetőek a lekritikusabb elemek. A Pareto diagram (4.2 ábra) jobban áttekinthető módon mutatja az eredményeket, ahol két elemi esemény kerül kiemelésre hasonló súlyozással:

5. rendszer specifikáció követelményeit hibásan kerül implementálásra;

illetve

3. hibásan implementált követelmények (interfész szempontjából).



4.2. ábra Pareto elemzés az elemi események bekövetkezése alapján

A kapott eredmény egyfajta megerősítése a módszer objektivitásának és az FMEA-t készítők következetes kiértékelésének, mivel a két kiemelt hiba redundánsnak tekinthető. Mind a kettő esemény a követelmény kezelésére vezethető vissza. Az LTFSM módszer ilyen fajta alkalmazása pedig a hibafa (FTA) már jól ismert alkalmazását tovább fejlesztve az FMEA-ból kinyert adatokkal kiegészítve a fejlesztési folyamatok jobbítására is alkalmazható. Feltéve, hogy az FMEA készítői egy adott hiba bekövetkezésének elkerülését vagy észlelhetőségét mérnöki folyamatok segítségével szeretnék biztosítani.

4.2 A hibamód és hibahatás elemzés érzékenység vizsgálata

Az érzékenység vizsgálatban célszerű elvonatkoztatni a kiegészítő információktól és csak a konkrét kockázati számokra fókuszálni. A vizsgálat célja a rendszer egészéhez képest vizsgálni egy-egy elem eltérésének a mértékét. A létrehozott mutatót érzékenységi együtthatónak nevezem, kiszámítása két lépcsőben történik. Először az egyes RPN számokhoz kerül viszonyításra az RPN számok összege, képletben kifejezve:

$$K_i = \frac{RPN_i}{\sum_{i=1}^{n} RPN_i} \tag{4.36}$$

A második lépésben az egyes kockázati számot alkotó tényezők eltérése a rendszer egészéhez viszonyítva kerül kiszámításra az érzékenységi együttható komponense:

$$K_{x_i} = x_i K_i, \text{ ahol } x \in \{S, O, D\} \tag{4.37}$$

Azonban felvetődik a kérdés, hogy az FMEA-ból kinyert adatokból készített hibafában elemezett érzékenységi vizsgálat és a forrásadatot szolgáltató FMEA érzékenységi vizsgálata hasonló eredményt szolgáltat-e. Elméleti síkon egy deduktív (FTA) és egy induktív (FMEA) érzékenységi elemzés kerül összehasonlításra.

A korábbi fejezetben bemutattam, hogy a hibafa alapú érzékenységi vizsgálat egy már ismert hiba (csúcsesemény) kialakulását vizsgálja az elemi és köztes hibák logikai kapcsolódásán keresztül, minden átmenethez egy valószínűségi értéket társítva. Egy-egy elemi hibához tartozó érzékenységi paraméter a logikai kapuk és a csúcseseményhez vezető él figyelembevételével számítandó.

Ezzel szemben az FMEA alapú érzékenységvizsgálat egy komplett rendszer mindhárom (S, O, D) értékelési eredményeiből indul ki. A pontozásokból számított kockázati számok a rendszer eloszlásához viszonyított számítására támaszkodnak. Elemzés eredményeként külön információ keletkezik a legsúlyosabb (S) kockázatot jelentő elemekről, a leggyakrabban előforduló (O) hibákról, illetve azok észlelési (D) hatékonyságáról.

Az előző fejezetben bemutatott hibafa érzékenységvizsgálathoz hasonló értékeket bemutató példa került felírásra a hibafa érzékenységi vizsgálatban használt értékeket átvéve az összehasonlíthatóság pontosságának megőrzése miatt.

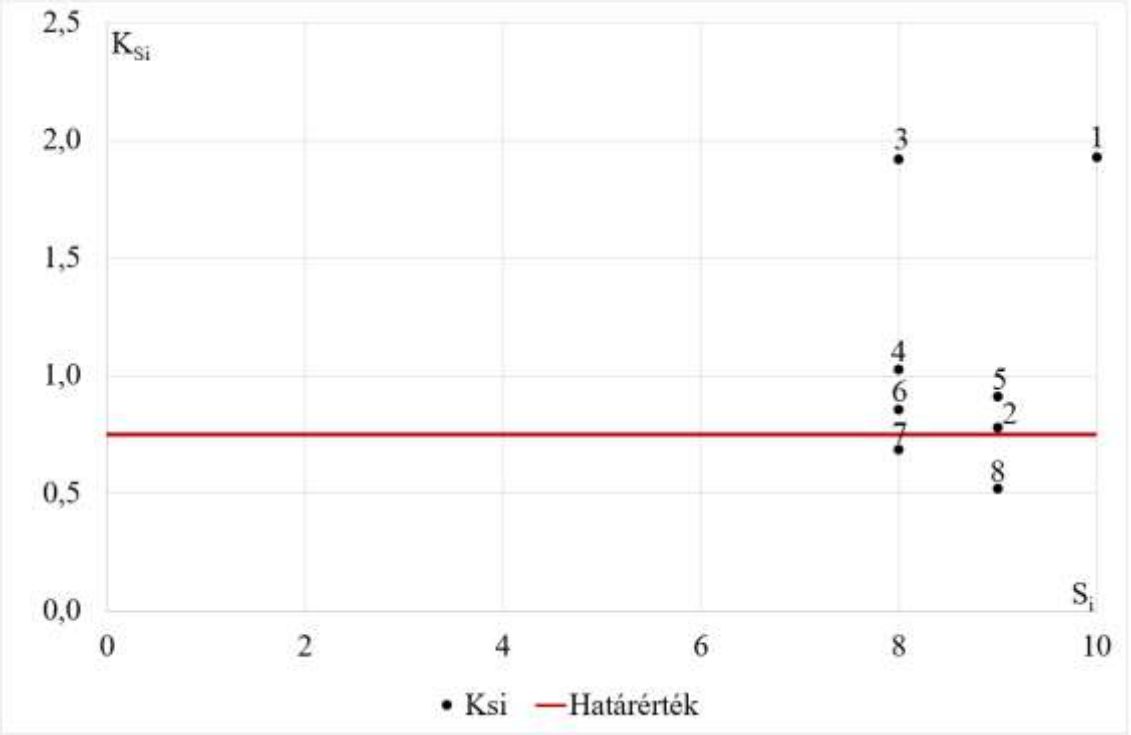
4.3 A hibafa és a hibahatás elemzés érzékenységének összehasonlítása

Az ismertetett K_i, K_{S_i}, K_{O_i} és K_{D_i} értékei kiszámítva láthatók a 4.2. táblázatban, ahol az *S, O, D* értékek rendre az FMEA súlyosság, előfordulás és észlelhetőség pontjai, míg az RPN ennek a három tényezőnek a szorzata. Egy sor egy funkcióhoz tartozó kockázati kiértékelést jelent. A K_i változó mutatja meg az eredő *RPN* értékhez viszonyított eltérését az adott elemnek. A K_{S_i}, K_{O_i} és K_{D_i} megmutatja az adott elem súlyossági (S), előfordulási (O) és észlelhetőségi (D) értékek *relatív eltérésének arányát* a rendszer eredő *RPN* kockázati értékéhez viszonyítva.

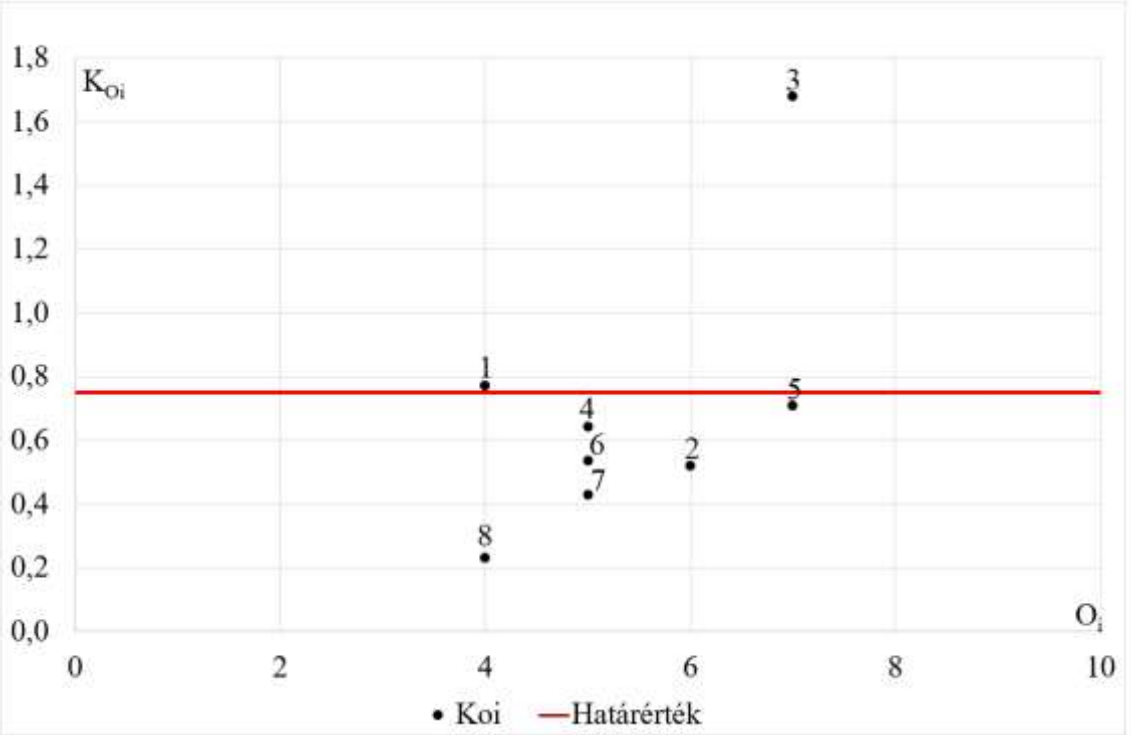
Ssz.	S_i	O_i	D_i	RPN_i	K_i	K_{S_i}	K_{O_i}	K_{D_i}
1	10	4	9	360	0,1928	1,9282	0,7713	1,7354
2	9	6	3	162	0,0868	0,7809	0,5206	0,2603
3	8	7	8	448	0,2400	1,9197	1,6797	1,9197
4	8	5	6	240	0,1285	1,0284	0,6427	0,7713
5	9	7	3	189	0,1012	0,9111	0,7086	0,3037
6	8	5	5	200	0,1071	0,8570	0,5356	0,5356
7	8	5	4	160	0,0857	0,6856	0,4285	0,3428
8	9	4	3	108	0,0578	0,5206	0,2314	0,1735

4.2. táblázat A kiszámított érzékenységi együtthatók és érzékenységi együttható komponensek

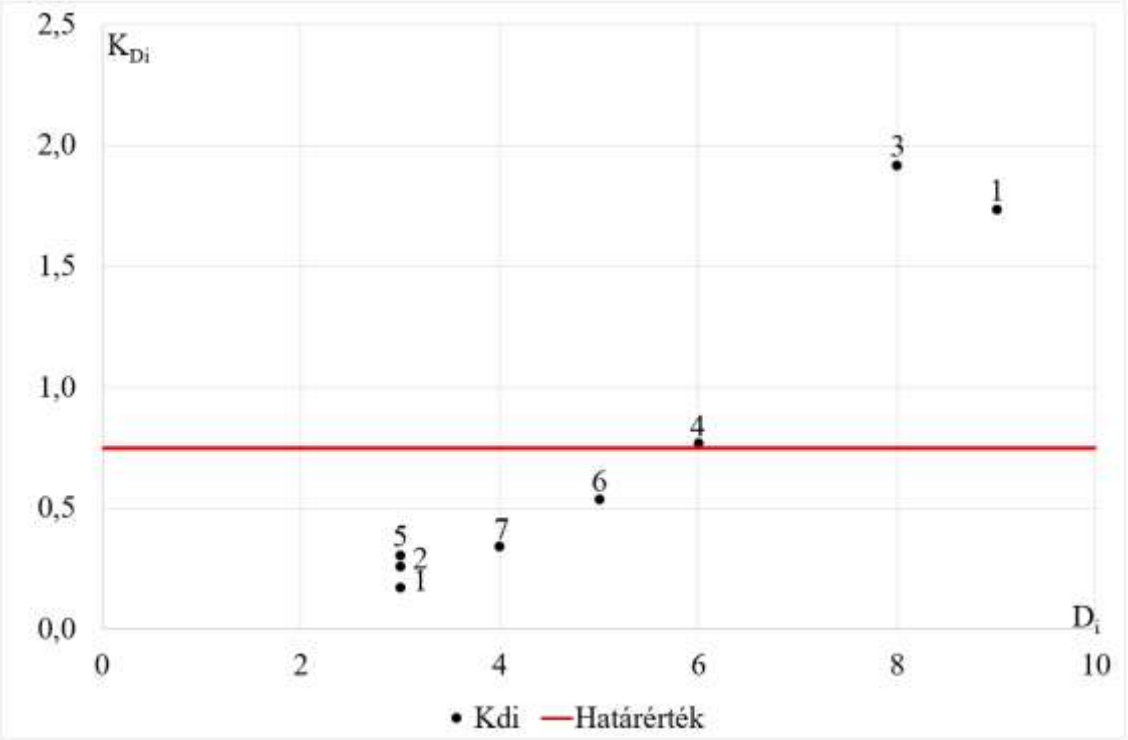
A kiszámított értékekből a grafikus koordináta rendszerben ábrázolva is látható, hogy ez a vizsgálat az 1 és 3 elemi eseményeket emelte ki.



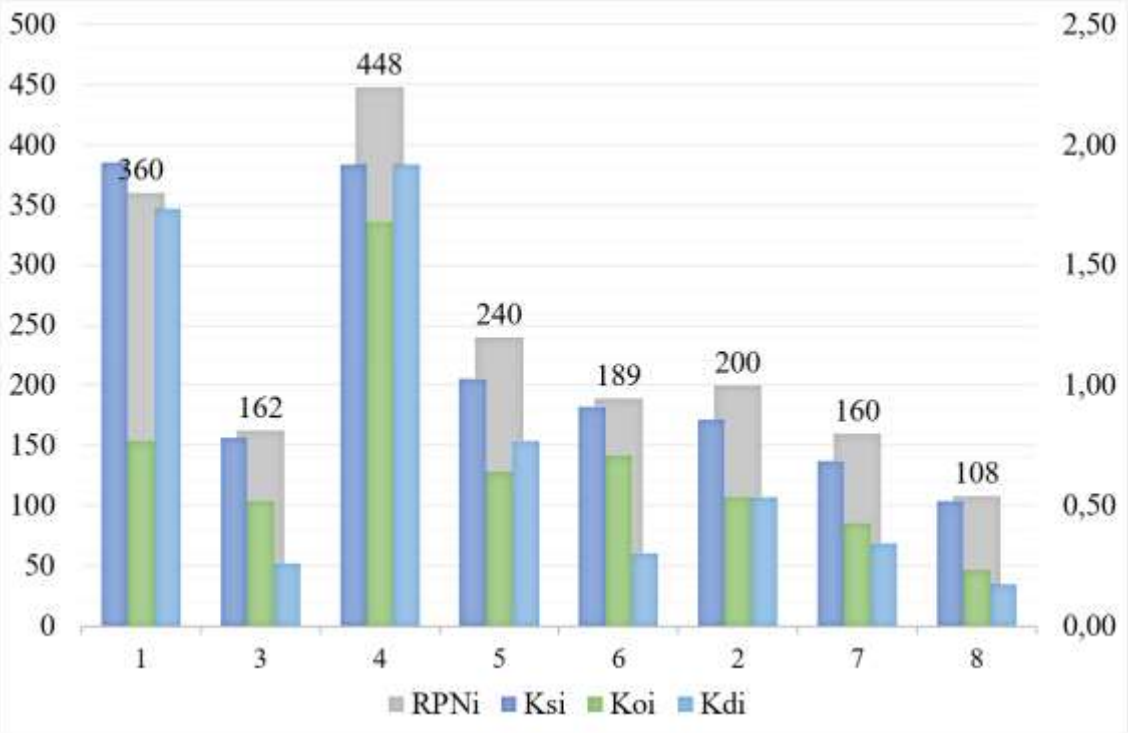
4.3. ábra A súlyosság (S_i) érzékenység elemzés eredménye



4.4. ábra Az előfordulás (O_i) érzékenység elemzés eredménye



4.5. ábra Az észlelhetőség (D_i) érzékenység elemzés eredménye



4.6. ábra A kockázati szám (RPN) és az érzékenységi mutatók összehasonlítása

Az ábrák kimagasló értékeket mutatnak az 1 és 3 hiba esetében, de a többi elem sem elhanyagolandó. Az eredmények betekintést engednek a kockázat megértésébe, hiszen a 4.3 ábrán látható a két nagyon kimagasló súlyosságú elemi esemény, amely még a 4.5 ábrán is kiemelkedő értéket mutat, míg a többi elemi esemény a határérték közelében marad. Felhívja a figyelmet ez a két kimagasló hiba, hogy az előfordulási lehetőséget csökkenteni szükséges, illetve minimum javítani célszerű a legmagasabb értéket képviselő hármas hibánál. Ez a csökkentés egy jól működő és hatásos méréssel várhatóan az észlelhetőséget is javítani fogja a 4.4 ábrán látható magas értéket csökkentve. Az első hibára viszont olyan intézkedés lesz szükséges, amely a könnyebben észlelhető, de ritkán előforduló hiba kizárását segíti. Ez ugyanis az egyik, de nem a legsúlyosabb hiba a 4.3 ábra alapján.

A példában látható kockázati számok és az érzékenységvizsgálat eredménye nagyjából megegyezik. Ez látható a hagyományos FMEA elemzésnél is, ahol szintén hasonló tendencia született az RPN szám és érzékenység függvényében. A hibafa elemzéssel összevetve, ahol az ötös és hármas eredmény került kiemelésre, addig itt az első és a hármas esemény. Az eltérés talán a hibafa alapjait jelentő deduktív elemzési alapokra vezethető vissza, mivel egy fő hiba felépülésének valószínűségét az elemi hibák logikai kapcsolatának ismeretében végzi el. Ezzel szemben az FMEA-ban viszont az egyes hibák egymástól független előfordulása, észlelhetősége van kihangsúlyozva a súlyosság és az egymásra hatástól függetlenül.

4.4 Következtetések, ajánlások

Ebben a fejezetben az alkalmazott érzékenységvizsgálatokat mutattam be és azok eredményeit hasonlítottam össze. Egy érzékenységi vizsgálat eredménye a rendszer stabilitása szempontjából a legkritikusabb lehetséges elemi hibákat tárja fel, illetve rangsorolja. A hibafa elemzésre épülő mátrixalgebrai vizsgálati módszer (LFTSM) felgyorsítja egy-egy vizsgálat lefolytatását és az elemi események kockázatának azonosítását. Az FMEA és a hibafa érzékenységi vizsgálatok eredményeinek összehasonlítása véleményem szerint nehézkes, mert a hibafa egy fő hibából indul ki, míg a hagyományos FMEA egy-egy külön hibát pontoz. A hibafa valószínűség számítási módszereket vesz alapul, míg az FMEA három különböző értékelési szempontot, Súlyosság (S), Észlelhetőség (D) és Előfordulást (O). A hierarchikus FMEA esetén viszont az egyik fő megkötés az adott hibának mindig ugyanazt a jelentéstartalmat és súlyosságot kell hordoznia

az egész rendszerben. Legfeljebb a kiváltó ok és előfordulás mértéke változhat funkcióról-funkcióra, amely finomíthatja egy hiba érzékenységre gyakorolt hatását. Ha egyetlen hiba kialakulásának okát szeretnénk mélyebben vizsgálni és a rendszerre gyakorolt hatását megismerni – máris előtérbe kerül a hibafa módszere.

Összességében, a relatív eltérések arányának vizsgálatában a rendszer eredő kockázati számához képest vizsgálom az adott funkcióhoz tartozó paraméter rendszerre gyakorolt hatását. Az eredményeket reprezentatív, könnyen áttekinthető grafikus formában, az összehasonlítást lehetővé tevő módon kerülnek ábrázolásra. Az FMEA-ból kiinduló elemzéssel a sokszor idő szűkében levő tesztelők, minőségbiztosítási szakemberek is áttekinthető képet kapnak a vizsgálandó rendszer gyenge pontjairól.

5 HIERARCHIKUS HIBAMÓD ÉS -HATÁS ELEMZÉS

Ebben a fejezetben az aktuális szabványokkal harmonizáló FMEA-ban alkalmazandó egységesíthető modellezési módszert mutatom be olyan elrendezésben, hogy az elemezendő rendszer tagolódásának megfelelően az egyes logikai szinteket hierarchikus elrendezésbe szerkesztem össze. A módszeremmel növelhető az így elkészült elemzés újrahasználhatósága, összehasonlítható az előrehaladás és a kidolgozottság szintje, illetve a logikai kapcsolatok követhetőek.

A hierarchikus jellegű, logikai sorrendbe rendezett FMEA nem új keletű ötlet, azonban az általam kidolgozott módszer a modellezés egységesítésében nyújt újdonságot egy multidiszciplináris (hardver-szoftver-mechanika) elemeket alkalmazó rendszerben. Célja a már említett egységes értelmezést úgy megvalósítani, hogy egy általános értelmezést nyújtson a rendszermodellezéséhez, ajánlást az adott szintek kialakításához. A módszer kidolgozásában fontos szempont az újrahasználhatóság az egyes rendszerelemek újra felhasználhatósága, változások követhetősége és az egyes diszciplínák igényeihez szükséges formátumok biztosítása.

5.1 A szintek felépítése

Az általam kidolgozott hierarchikus FMEA (röviden H-FMEA) a klasszikus hármas tagozódást veszi alapul a hatás-funkció-ok (effect – function – cause). A hierarchia két végén egy-egy, szinte katalógusnak is használható elemzés áll nem teljes értékű kiértékeléssel. A legfelsőbb szintet „effect level” azaz „hatás szint”-nek nevezem a termék azon funkcióit vagy tulajdonságait a vevő számára, amelyeket észlelhet. Az egyes funkciókból adódó lehetséges meghibásodások hatásai és a hozzá tartozó súlyosság kerülnek kiértékelésre. A kiértékelt hibahatások okait az egy szinttel lentebb található rendszer FMEA-kban elemzik ki. Az adott hibahatáshoz tartozó alrendszer viszont a hatás szinten a „hiba oka”-ként kerül feltüntetésre, mint a hiba létrejöttében érintett elem. A hatás szint alkalmas arra is, hogy itt kerüljön olyan hibamód vagy hibahatás definiálásra, amelyet egy korábbi elemzésből, vagy előírásból szükséges feltüntetni. Végigvezetve a felírt hibát a releváns funkciók megfelelő pontjaira a hierarchikus logikai kapcsolatban felépített FMEA-n lehetségessé válik azonosítani a definiált elemek hatását a hozzájuk tartozó súlyosság (S) értékkel a rendszer egészére nézve. Hasznos lehet például az autóiparban, ha a funkcionális biztonság (ISO 26262) szabványból adódó „top hazard”-okat, (az elkerülendő veszélyes hibákat) bizonyítani tudják, hogy a rendszer funkcióiban megvizsgálva kezelik a kockázatokat, tehát

figyelembe vették a rendszer- és a tervezési szintek kockázati elemzésében. A hatás szint tehát kiváló áttekintést nyújt a rendszerben előforduló hibákról és súlyosságáról (S). A súlyossági paraméter (S) módosítása csak a projekt csapat és vevő jóváhagyásával lehetséges. A szint létrehozásával könnyen áttekinthetővé válik a rendszerben elemezett, előforduló hiba hatások listája.

5.2 A hierarchia felépítése

Az első szint, amely teljes kiértékelést tartalmaz ez a rendszer szint, ahol a rendszer FMEA-k kerülnek kiértékelésre. Ezekhez a szinthez kapcsolódnak az egy szinttel lentebb található konstrukciós FMEA-k, amelyek szintén teljes értékű kiértékelést tartalmazhatnak. A speciális karakterisztikák kezelése szintén ezen a rendszer szinten kerül felvezetésre, noha az [47] referencia könyv szerint azt a konstrukciós szinten kellene megoldani. Ennek azaz oka, hogy ebben a modellezési ajánlásomban a konstrukciós szinteken sokkal inkább a termék tervezési hibái kerülnek kielemzésre, míg a karakterisztikát jelölő minősítés a logikai kapcsolattal kerül rögzítésre a fentebbi szinten. Egy esetleges alkatrész visszavonása a speciális karakterisztika törlésével is járhat, amelyről a fejlesztői részleg elfeledkezhet, de a gyártásban és a Control Plan-ben jelentkezik ez a probléma. Ezért a karakterisztikát célszerű így rögzíteni, hogy egy esetleges módosítás miatt a design FMEA-ban csak az adott méret rögzítése látható és ez eltűnhet egy munkalap visszavonásával. Azonban egy szinttel feljebb a funkció vagy más tulajdonság feltüntetése mellett látható a speciális karakterisztika indoka is. A javasolt, alkatrésztől független bejegyzés ugyancsak támogatja, ha esetleg időközben új anyag bevezetése válik szükségessé, könnyebben követhető az aktuálisan használt alkatrészlista és a bevezetés indoka is követhető.

A hardver és a mechanikai FMEA-k alkatrészei egy nagyobb funkció csoport szerint kerülnek hierarchiába rendezve. Ez azt jelenti, hogy a rendszer FMEA szintjén egy funkció (pl. tömítés) kerül felvételre és az ezalatti szinten lesznek ennek a funkciónak a működtetésében résztvevő alkatrészek felsorolva. Az alkatrészeknél előfordulhat, hogy több helyre is bekerül ugyanaz az elem, amely adatduplikálódást jelent ugyan, de az érthetőséget, követhetőséget javítja. Ezt a kísérletben használt, Plato AG által forgalmazott Scio rendszerben a „linkelés” funkció segítségével lehetséges megoldani. Ez azt jelenti, hogy az eredeti elemzés példányához hozzá lesznek kapcsolva a további helyekre bemásolt elemek. A linkelés pedig biztosítja, hogy a többi helyen feltüntetett alkatrész minden helyen pontosan ugyanazt az információt tartalmazza, ha módosítják a tartalmát, akkor a módosított tartalom megjelenik minden példányban, hiszen ugyanarról az elemről van szó.

A konstrukciós szint eltérő tartalmú az elektronikus hardver komponensek tekintetében, egy-egy alkatrész meghibásodását célszerű vizsgálni (ahogyan az korábban is említésre került a 3. fejezetben). Azonban a tradicionális elemzéstől eltérés, hogy a funkcióba rendezés a csoportosítás alapja a mechanikai FMEA-hoz hasonlóan. Például egy tápegység az ECU[9] számára lesz egy rendszer szint, majd alatta felsorolásra kerül az azt felépítő alkatrészek, ellenállások, kondenzátorok, stb.. Az elemzési lánc legvégén egy szinttel lentebb az „ok" gyűjtemény (cause) kerül, ahol a kiváltó hiba okok vannak felsorolva. Ezeket lehet később az elemzést megkönnyítő hibagyűjteményként alkalmazni és újra felhasználni. A fentebb ismertetett indok miatt a speciális karakterisztika most sem kerül felvezetésre, miszerint az elektronikus alkatrészeket többször is megvizsgálják a gyártás folyamán – meggyőződve azok helyes értékéről, méretéről és beültetéséről.

A mechanikai FMEA-k tekintetében általános, minden alkatrészre alkalmazható sablon került megfogalmazásra, amely tárgya lehetne akár egy tervezési ellenőrzésnek is. A cél a készülő termék kockázatának kiértékelése és nem pedig az adott tervező munkájának bírálata. Így jobban tudnak egyre inkább elvonatkoztatni és az elkészült mintára, a tervezési aspektusokra és funkcionalitásra fókuszálni. A megfogalmazott szempontok az alábbi csoportokba sorolhatók:

- Meggyőződni a megfelelő anyagválasztásról.
  (Dilatációs koefficiens, keménység, alkalmazási osztály, gyártási technológia, stb.)
- Meggyőződni a megfelelő geometriai paraméterekről.
  (Magasság, mélység, átmérők, rugó paraméterek, zsírozási zóna, stb.)
- Meggyőződni a megfelelő felületi definíciókról.
  (Felületi bevonat, keménység pontossági osztálya, fúrási irány, stb.)
- Meggyőződni a kötődő komponensek megfelelő kapcsolódásáról.
  (Rögzítés típusa, száma, ereje, sorrendje, nyomatéka, stb.)

A szoftverek tekintetében pedig a már említett három szint: platform, adatközvetítő réteg, rendszer/logika szint kerülnek elemzésre. Az eljárás csak rendszer szintű FMEA-kat alkalmaz, ahol a szoftverek moduljai egy-egy FMEA munkalapot foglalnak el. Célszerű a

[9] Electronic Control Unit: az autóiparban használt általános kifejezés, a gépjármű egy vagy több egységét vezérlő elektronikát foglalja magába.

„szürke doboz[10]” módszerét alkalmazni és nem csupán a követelményekre támaszkodni. A számos ellenőrzés (review) és tesztelés ellenére is érdemes figyelmet fordítani a szoftverek funkcióinak elemzésére és a kockázat kiértékelésére, megelőző akcióként definiált vizsgálatokkal pedig kizárni az egyszerű, de kellemetlen hibaforrásokat, mint például a nullával való osztás előfordulását. Az egyes funkciók működésének biztosításáról is célszerű meggyőződni, hogy a bemenetre érkező paraméterek használhatóak és nem idéznek elő kritikus működést. Erről célszerű meggyőződni akár egy hitelességi (plausiblility) vizsgálattal. Megvizsgálni az egyes műveletek elvégzését, amely egy termék érettségi szintet lezáró minőségügyi ellenőrzőlista része is lehet. Tapasztalatom szerint érdemes újra átgondolni ezeket és az FMEA-ban is rögzíteni, hiszen a követelmények és a tervek együttes kockázati kiértékelése itt kerül dokumentálásra.

Fontosnak tartom a megbeszéléseken résztvevők tapasztalati és szakterületi ismeretének figyelembe vételét a megfelelő összetétel megfelelő kialakításához. Erre hívja fel a figyelmet Hu Chen is [53] cikkében, ahol a kockázat kiértékelését a résztvevők tulajdonságai alapján súlyozza konszenzus, hezitálás, illetve a többség véleményének tükrében. Azonban a csoport összeállításánál inkább a szakmai és a projektbeli szerepkör mérvadó azért, hogy a hatékonyságot maximalizálhassuk az amúgy is kapacitást és időt igénylő megbeszélésen. Az általam szervezett és moderált megbeszéléseken általában két fejlesztőt hívtam meg. Az egyik a forráskódot készítő, míg a másik a fejlesztő, aki az adott modult ellenőrizte (review). illetve így mind a ketten ismerték a funkciókat. A funkciók és hibamódok felvételét követően egy tesztelőre is szükség volt, aki az előfordulási gyakoriságot (O) segített megállapítani, illetve tapasztalatai alapján az észlelhetőséget (D) is. A tesztelő a funkciók felvételekor nem volt jelen, mivel a tesztelés miatt nem célszerű, hogy ilyen mélységben ismerjen egy adott modult, befolyásolva a gondolkodását az adott vizsgálandó egységről. Így viszont a pontozással is legfeljebb „szürke dobozként” tud a termékre tekinteni.

A kidolgozott módszertannal sikerült felére rövidíteni az FMEA-ra fordított időt az előzetes, sablon rendszerű formátummal, csökkentve a kezdeti próbálkozások számát. A fejlesztő mérnökök számára elgondolkodtató és hasznosnak bizonyuló eredmények felmutatásával javult az elemzés készítésének hasznossági megítélése. Általánosságban felvetődő témák például egy funkció robusztusabbá tételének a bizonyított igénye, egy

[10] „Szürke doboz” módszere esetén a rendszer be és kimenetét, illetve főbb funkcióit ismerjük, a részletes működés rejtve marad.

elmaradt használati eset (use case) kidolgozásának hiánya, stb. volt. Az elemzésben való részvételi hajlandóság javulását is egy kézzel fogható eredménynek tartom, mert sajnálatos tapasztalat, hogy a FMEA készítése nem a legfontosabb teendők között szerepel. A szoftveres moduloknál az elemzést egy második szintű ellenőrzésnek tekintették kezdetben. A megbeszélésen a fejlesztők egy rendszerbe integrálva láthatták a modulokat, olykor olyan információkat megismerve, ami a követelmény menedzsmentből nem kaptak meg. A szoftver architektúrával ellentétben itt a hardver és mechanikai komponensek is megtalálhatóak. Egyik legszembetűnőbb eredményt jelentette, amikor az egyik megbeszélésen szembesült a fejlesztő azzal, hogy az általa fejlesztett modul áttervezésre és kiegészítésre szorul a megbízhatóbb működés elérése érdekében. Egy ilyen eredmény elérését követően ugyancsak megtapasztalhatóvá vált a kiértékelés finomításának igénye is.

5.3 Következtetések, ajánlások

Ebben a fejezetben bemutatásra került az FMEA-k hierarchikus jellegű elrendezése, amelyet H-FMEA néven ismertettem. Hangsúlyoztam, hogy nem egy újkeletű ötletről van szó a hierarchikus elrendezést illetően, de ennek a sematizálása és a kockázati számok öröklődésének biztosítására megoldást jelenthet. A VDA, AIAG szabványok, amelyek autóiparban FMEA releváns ajánlásokat közölnek mégsem adnak előírást a hierarchikus elv alkalmazásának minél optimálisabb gyakorlatára (best practice). A felismerés, hogy az egyes mechanikai elemek analízisénél ne a tervező munkájának megoldási szintje kerüljön pontozásra, hanem a követelmények fényében elvégzett tervezési aspektusok összegzése, feltehetően a konstruktőrök számára is jobb megoldás. A gyártás számára releváns speciális, SPC karakterisztikák kezelését is új módon javasolom megoldani, hiszen a változással, egy FMEA munkalap visszavonásával törlődhetnek fontos információk. Az egy szinttel feljebb helyezéssel viszont egy törléssel megmarad a forrásinformáció, hogy mi alapján került felhelyezésre a karakterisztika és a helye is. A katalógus elv segítségével a korábbi tapasztalatok (Lessons Learned) újbóli felhasználását támogatom, amellyel gyorsíthatók az elemzésre szánt idők. Az elméleti leírással bemutatott H-FMEA alkalmazási lehetőségét a következő fejezetben szemléltetem egy esettanulmányon keresztül.

6 HIERARCHIKUS HIBAMÓD ÉS -HATÁS KOCKÁZAT KEZELÉSE ÉS ÉRZÉKENYSÉG VIZSGÁLATA

Egy elem vagy funkció kockázatának kiértékelése egyértelmű feladat az FMEA-ban, hiszen három tényező szorzata: a súlyosság (S), az előfordulás (O) és az észlelhetőség (D) szorzata teszi ki a kockázati számot (RPN). Jelenleg az RPN mértéke határozza meg az adott elemhez tartozó kockázat szintjét, a tényezők értékének meghatározását katalógusok segítik például: SAE J1739, QS9000 vagy VDA, stb.. Azonban a szorzás kommutatív tulajdonsága miatt a kockázati szám eltérő súlyosságú, elfordulású és észlelhetőségű esetekre is azonos RPN értéket adhat. Gondoljunk bele a 10x2x5 vagy 2x10x5 esetekbe, ahol súlyosság - előfordulás - detektálhatóság sorrendben írjuk fel a pontszámokat. Az első esetben látható, hogy egy súlyosnak osztályozott esemény, ami alig fordul elő és közepesen észlelhető, azonos kockázati értékkel rendelkezik, míg a második kevésbé súlyos, de nagyon gyakran előforduló és nehezen detektálható esemény. A kockázat kiértékelésével kapcsolatos publikációkban néhány példa látható arra, hogy a kiértékelő mérnöki csoport résztvevőinek tulajdonságait is figyelembe veszik súlyozásként egy döntéstámogató módszert, a PROMETHEE-t (Reference Ranking Organization Method for Enrichment Evaluations) alkalmazva [46] [42]. Máshol a Fuzzy elméletet vonják be a kiértékelésbe vagy éppen egy újabb szempont szerint súlyozzák vagy rangsorolják a meglevő kockázatokat pl. kockázat alapú tesztelésnél [62] [84].

Hu-Chen Liu, Wenyan Song és Quian Su cikkükben [65] az FMEA csapat tagjainak egyéni tulajdonságait is figyelembe veszik egy kockázat meghatározásánál, például: mérlegelés foka (hesitation degree), egyetértés szintje (consensus degree), illetve az összes adódó más egyéni emberi tényező befolyásolását és a nyelvi megfogalmazást (linguistic terms). Véleményük szerint minél kisebb a mérlegelés ideje egy résztvevőnek, annál pontosabb az információ, amely által az adott munkatárs súlyát növelik a csoport tagjaihoz képest. A nyelvi kifejezésekből generált felhő súlyozása aggályos lehet, hiszen nem tűnik egyértelműnek két FMEA rendszerének összehasonlíthatósága műszaki kidolgozottság és tartalom szempontjából, mivel más szakszavakat használ a szoftver és másokat a mechanika. Összességében azonban jelentősen függ a kidolgozás nyelvétől. Ugyanakkor a követelménykezelési módszertan az Interantional Requirement Engineering Board (IREB) hasonlóan alkalmazza a szavak elemzésén alapuló módszert főként angol nyelvi területre

építve, minimum mondatelemeket meghatározva egy-egy követelmény minimum tartalmaként: például ige, tárgy, szám és mértékegység. Azonban ez a módszertan sokkal inkább az egyes követelmények teljességére irányul, mintsem a kidolgozottságra és logikai kapcsolódásra. [70] Ezért nem érdemes véleményem szerint megállni egy-egy elem elemzésénél, hanem egységes sablonokat célszerű figyelembe venni adott diszciplína igényének megfelelően, majd azokat összekapcsolni. Rugalmasságot és valamennyi mozgásteret hagyva a projekt egyéni igényeinek, de előnyös, ha már maga a sablon lehetőséget ad egyfajta logikai kapcsolatok létesítésére.

A VDA munkacsoport 2018-as összefoglalója szerint [88] a „Design FMEA Action Priority (AP)" bevezetését javasolja az RPN kiegészítésére. A tervezet szerint az egyes összetevők (S, O, D) adott tartomány közötti értékeinek függvényében alakítják ki a végső AP szintet, amely H – high, M-medium és L-low lehet. Ugyancsak megjelenik a „Monitoring and System Response" fejezet, amelyben a rendszer válaszát és a biztonsági (safety) előírások teljesülését is figyelembe veszik a súlyozásnál. A kiértékelési katalógusban a biztonsági (safety) előírások teljesülését értékelik ki, amelyek csak H-high vagy L-low értékelést kaphatnak.

A funkciók kockázatának ismeretével következtetni lehet egy rendszer sérülékenységére, gyengepontjaira, amelyek veszélyeztetik a stabil állapot fenntartását. Célszerű tüzetesebben átvizsgálni és tesztelni ezeket, hogy mennyire működnek ezek a kritikus pontok robusztusan és megbízhatóan. Az FMEA eredményeinek grafikus vizsgálatára alkalmazható a Pareto elemzés, hogy kiemeljék az RPN szám alapján azonosított gyenge pontok eloszlását. Azonban látható, hogy a kiértékelés értelmezése sokszor mégis finomításra szorul, ezért célszerű egy nagy FMEA rendszer elemeinek kiértékelését lehetőség szerint automatizálni, feldolgozni és prezentálható formába önteni. Elvonatkoztatva az FMEA hagyományos kiértékelési módszereitől, az FMEA-ból kinyerhető eredményeket fölhasználó kvalitatív analízist, a hibafa elemzés felhasználásával ismertettem korábban egy érzékenységvizsgálatot, míg a következőkben az FMEA kockázati értékelését finomító érzékenységi vizsgálatot mutatom be.

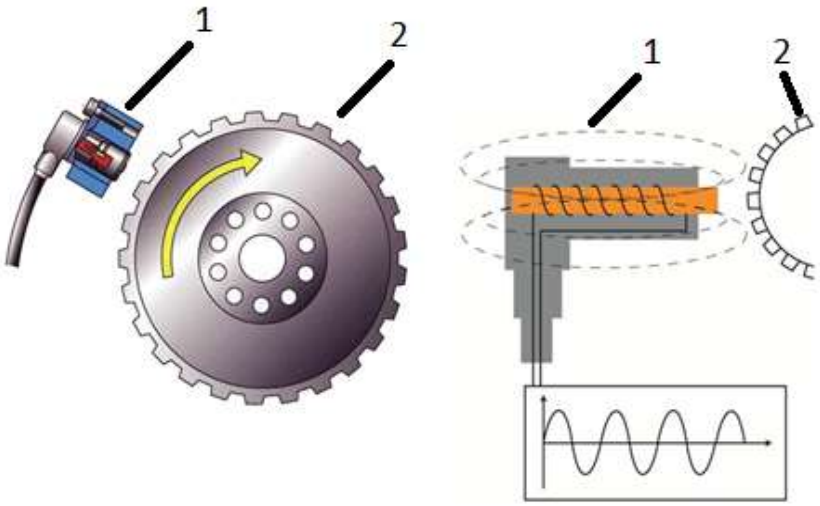
S	O	D	AP	AP indoklása
9-10	6-10	1-10	H	Magas prioritású a biztonsági és/vagy szabályozási hatások miatt, amelyek magas vagy nagyon magas előfordulási gyakorisággal rendelkeznek.
9-10	4-5	7-10	H	Kiemelt fontosságú a biztonsági és/vagy szabályozási hatások miatt, amelyek mérsékelt gyakorisággal rendelkeznek.
5-8	4-5	5-6	H	Kiemelt fontosságú az alapvető vagy kényelmi járműfunkció elvesztése vagy csökkent működése miatt, amely mérsékelt előfordulási gyakorisággal és mérsékelt észlelhetőséggel rendelkezik
5-8	4-5	1-4	M	Közepes fontosságú az alapvető vagy kényelmi járműfunkció elvesztése vagy csökkent működése miatt, amely mérsékelt előfordulási gyakorisággal és alacsony észlelhetőséggel rendelkezik
2-4	4-5	5-6	M	Közepes előfordulási gyakoriság a mérhető minőség (megjelenés, hang, heptika) miatt, mérsékelt előfordulási gyakorisággal és mérsékelt észlelési minősítéssel rendelkezik.
2-4	4-5	1-4	L	Alacsony előfordulási gyakoriság a mérhető minőség (megjelenés, hang, heptika) miatt, mérsékelt előfordulási gyakorisággal és alacsony észlelési minősítéssel rendelkezik.
1	1-10	1-10	L	Alacsony prioritás a nem észlelhető hatás miatt.

6.1. táblázat Az Action Priority pontozása – Design FMEA szintjén forrás (VDA) [88] alapján

Action Priority (AP)	Cselekvési elvárás
Magas	A csoportnak meg kell határoznia egy megfelelő megelőzési módszert, hogy fejlessze az észlelést és/vagy az észlelés ellenőrzésének javítását célzó megfelelő intézkedést vagy észlelést. Ezt dokumentálnia és igazolnia kell, hogy a jelenlegi ellenőrzések megfelelőek.
Közepes	A csoportnak meg kell határoznia megfelelő intézkedéseket a megelőzés és/vagy észlelés ellenőrzésének javítása érdekében, vagy a vállalat megítélése szerint igazolja és dokumentálja, hogy az ellenőrzések megfelelőek.
Alacsony	A csapat azonosítani tudná a megelőzés vagy észlelés ellenőrzésének javítását célzó intézkedésesüket.
Ajánlott, hogy a potenciális súlyossági érték (9-10) hibahatásait, az Action Priority magas és közepes értékei esetén legalább az eddig definiált cselekvési terveket a menedzsment ellenőrizze le.	
Itt nem egy olyan rangsorolásáról van szó, hogy „Magas”, „Közepes” vagy „Alacsony” kockázat. A kockázatok csökkentésére irányuló intézkedések szükségességének prioritása.	

6.2. táblázat Az Action Priority kiértékelése (VDA) [88] alapján

A jobb érthetőség érdekében a vizsgálat egy ismert rendszer, az Anti-Block System (ABS) egyik komponense, a keréksebességmérő (Wheel Speed Sensor – WSS) szenzor elemzési példáján kerül bemutatásra. A jármű kerékforgási sebességéről, illetve aktuális mozgási állapotáról szolgáltat információt ez az eszköz. Két alkatrészből épül fel: egy induktív szenzor és egy fogaskerék alkotja. Működését tekintve a jármű kerekére rögzített fogaskerék forgásával egy periodikus jelet állít elő, melyből a jármű sebességének változására lehet következtetni. A jármű összes kerekére rögzítésre kerül ez az eszköz, felépítése a 18. ábrán látható. [85][7]



6.1. ábra Keréksebességmérő érzékelő felépítése és működési elve [85]

1 – Induktív szenzor ; 2 – Fogazott kerék

6.1 A hagyományos FMEA érzékenységi együtthatóinak meghatározása

A termékre készült, egy szinten elemzett hibamód és -hatáselemzés (FMEA) a 6.3 táblázatban látható. A berendezés két fő feladata egy periodikus jel előállítása és annak változtatása az abroncs forgása alapján. Azonban a 6.3 táblázat tovább olvasásával látható, hogy nem csupán a kerék sebességének vizsgálatára használják ezt a jeladót, hanem a mért adatokból következtetnek az adott abroncs blokkolt vagy guruló állapotára is. A kiváltó okok között előtérbe kerülnek az alkotóelemek meghibásodásai, amelyek jellemzően a hardverre visszavezethető meghibásodást tartalmaznak. A táblázat minden sora kiértékelésre került, így megelőző és észlelő intézkedések, amelyek csökkentik a kockázati számot (P és D feladatok).

No.	Funkció	Pot. hiba	Pot. hiba hatása	*S*	Hiba oka	*O*	Prev./ Det. Akció	*D*	*RPN*
1	Periodikus jel előállítása a kerék forgása alapján	Periodikus jel eltér a kerék sebességtől	Rossz sebességi érték	7	A jeladó folyamatosan fémet érzékel	4	D: Ellenőrizni a kábel köteget P: Vízálló technológia használata	2	56
2			Rossz sebességi érték	7	Fogaskerék fogai között nem egyenletes a távolság	2	D Ellenőrzés egy másik szenzorral P: Előírni időszaki ellenőrzést a fogaskerékre	3	42
3		Nem továbbít jelet	Sebesség nem meghatározható	10	A jeladó nem érzékel fémeket	3	D: ellenőrizni az értékek hitelességét P: Meggyőződni a szenzor megfelelő rögzítéséről	3	90
4		Kerék blokkolása nincs észlelve	Hibás érték a blokkoló kerék állapotáról	8	Fogaskerék fogai között nem egyenletes a távolság	2	D: Gyártási audit P: Meggyőződni EoL méréssel	2	32

6.3 a táblázat A WSS rendszer hagyományos FMEA elemzése

No.	*Funkció*	*Pot. hiba*	*Pot. hiba hatása*	*S*	*Hiba oka*	*O*	*Prev./ Det. Akció*	*D*	*RPN*
5	Periodikus jel frekvenciájának változtatása a kerék sebessége alapján	A kerék állapotát állónak érzékeli guruló állapot helyett	Hibás érték a blokkoló kerék állapotáról	8	A jeladó nem érzékel fémeket	2	D: Ellenőrizze a gyújtást is P: Ellenőrzés egy másik kerékkel	3	48
6					A jeladó folyamatosan fémet érzékel	2	D: Aperiodikus jel felismerése P: Meggyőződni a szenzor megfelelő rögzítéséről	3	48
7		A kerék állapotát gurulónak érzékeli álló állapot helyett	Jármű instabillá válik	9	Folyamatosan fém jelenlétét mutatja a szenzor	1	D: Összehasonlítás egy másik kerék állapotával P: Meggyőződni a szenzor megfelelő rögzítéséről	2	18

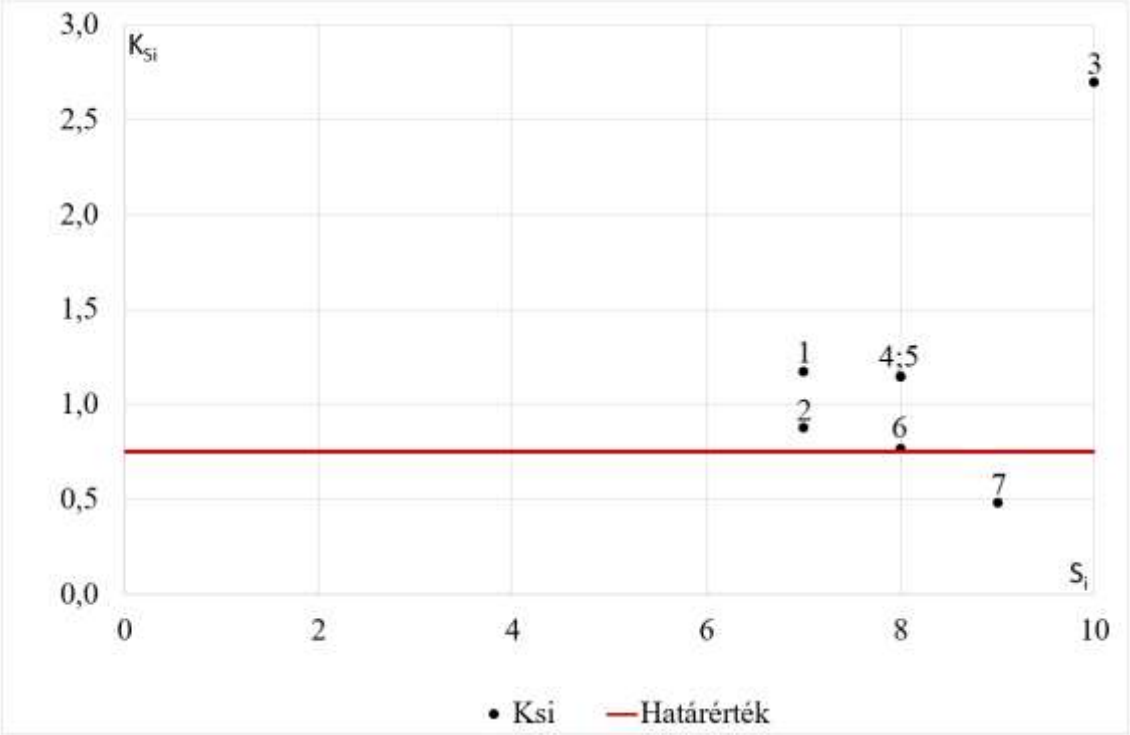
6.3 b táblázat A WSS rendszer hagyományos FMEA elemzése

Az ismertetett K_i, K_{S_i}, K_{O_i} és K_{D_i} értékei kiszámítva láthatók a 6.4 táblázatban.

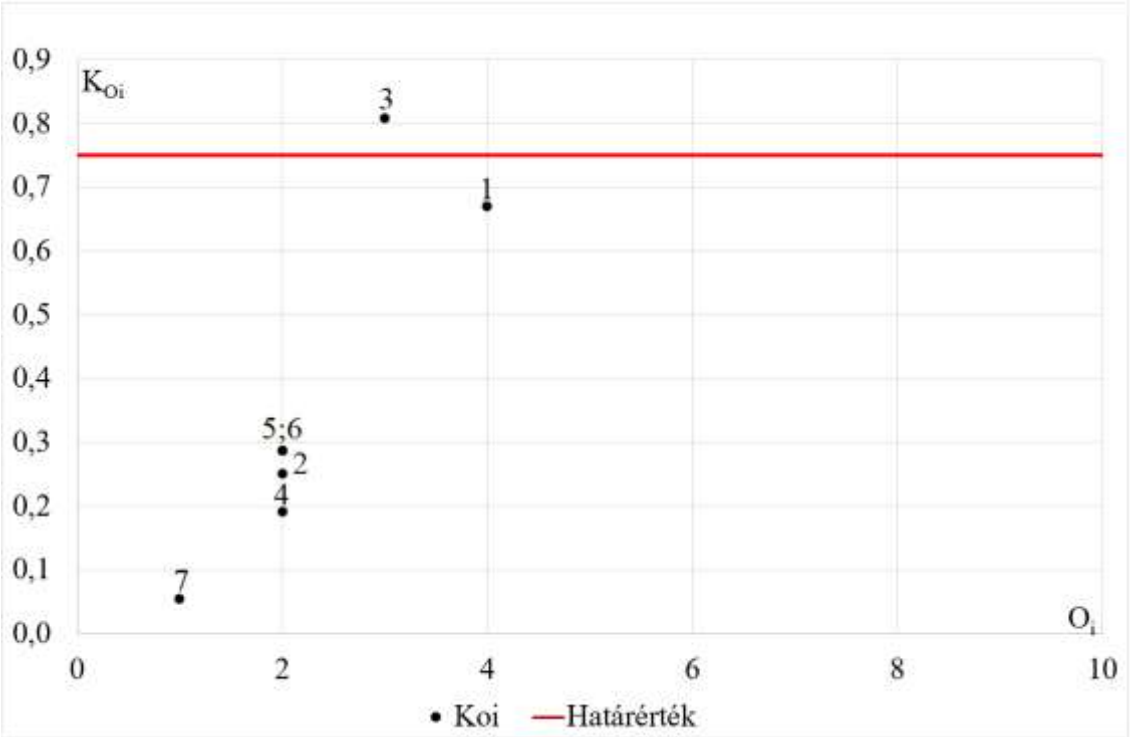
No.	S_i	O_i	D_i	RPN_i	K_i	K_{S_i}	K_{O_i}	K_{D_i}
1	7	4	2	56	0,1677	0,1737	0,6707	0,3353
2	7	2	3	42	0,1257	0,8802	0,2515	0,3772
3	10	3	3	90	0,2695	2,6946	0,8084	0,8084
4	8	2	2	32	0,0958	0,7665	0,1916	0,1916
5	8	2	3	48	0,1437	1,1497	0,2874	0,4311
6	8	2	3	48	0,1437	1,1497	0,2874	0,4311
7	9	1	2	18	0,0539	0,4850	0,0539	0,1078

6.4. táblázat A kiszámított érzékenységi együtthatók és érzékenységi együttható komponensek

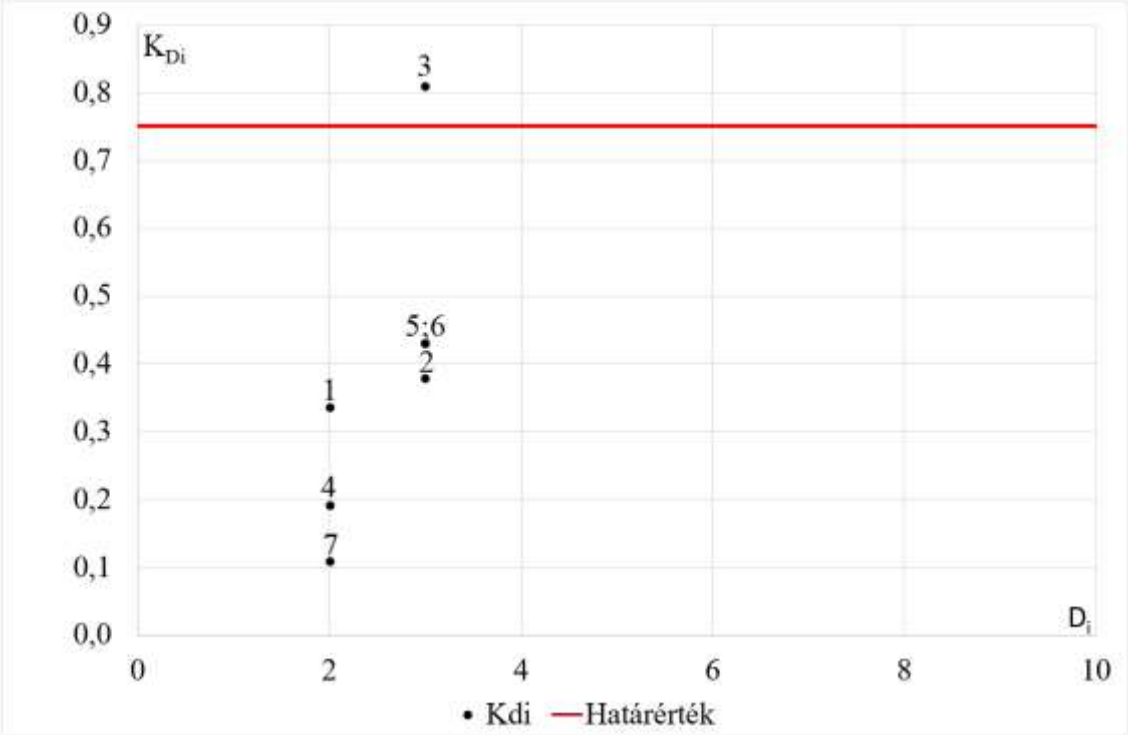
Az értékek grafikus ábrázolásával könnyen áttekinthetővé és prezentálhatóvá válnak a korábban készített FMEA elemzés eredményei. A grafikonon egy határértéket határoztam meg, amelyet tapasztalati úton választottam, hogy jobban kiemelje mely esetekkel célszerű foglalkozni. Az első grafikon a súlyosság (S) értékhez viszonyítva, a második az előfordulás (O), a harmadik az észlelhetőség (D) érzékenységi együtthatóit mutatja be a 6.2-6.9 ábrákon.



6.2. ábra Súlyossági érzékenységvizsgálata



6.3. ábra Előfordulási érzékenységvizsgálata



6.4. ábra Észlelhetőségi érzékenységvizsgálata

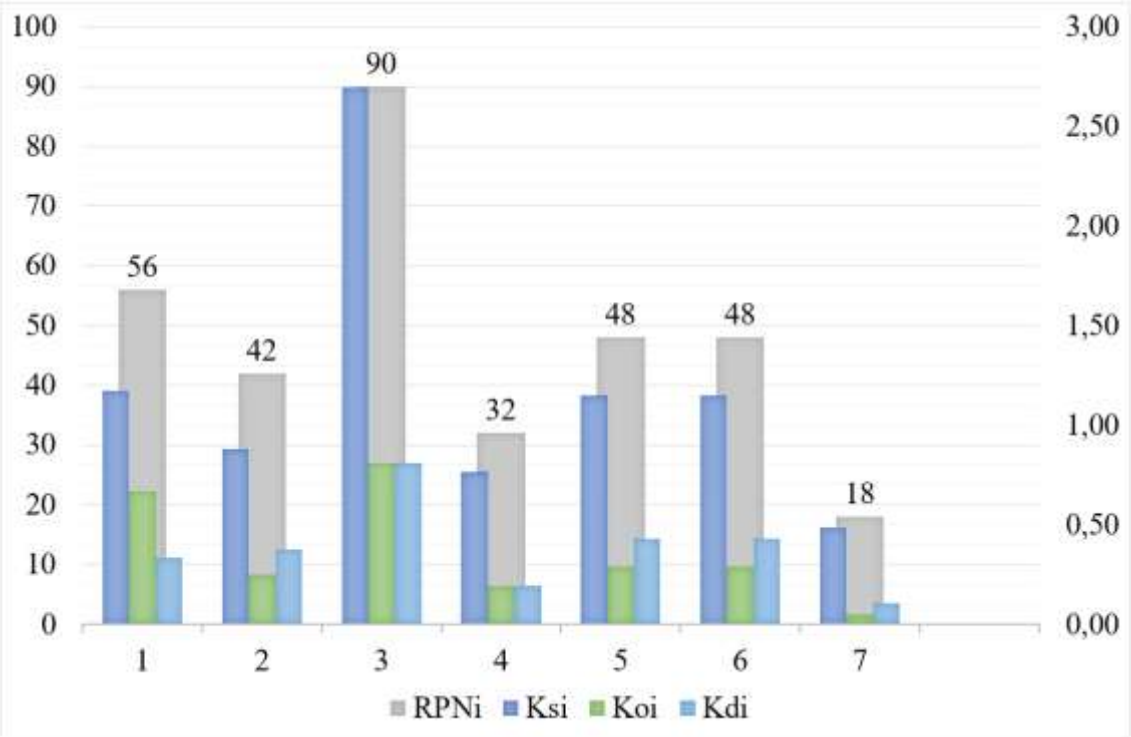
A súlyossági grafikon (6.2. ábra) azt mutatja, hogy a vizsgált rendszer funkciói többsége igen súlyos hatásúak. Ez azt az üzenetet hordozza, hogy érdemes döntést hozni, hogy a funkciók mennyire tekinthető kritikusnak a rendszer egészére nézve. A termékbiztonsággal és megbízhatósággal foglalkozó szakembereknek érdemes mérlegelni, hogy valamilyen minőségbiztosítási eszközzel vagy műszaki megoldással növeljék az adott elem megbízhatóságát, illetve csökkentsék a már nem elfogadható kockázatot. A legveszélyesebb eset az, ha a jeladó nem ad jelet a jeladó, amely magasan kiemelésre került. Belegondolva a jármű dinamikájába a stabilításáért felelő egyik fő funkció például az Electronic Stability Program (ESP), amely a jármű mozgásának függvényében végez korrekciókat az abroncsok egyedi sebessége alapján, hogy megakadályozza minden egyes csúszásból eredő kontrollálhatatlan állapot kialakulását. Ez a funkció fékerőt is kivezérelhet a kerekekre külön-külön, amely jelentősen befolyásolja a jármű stabilitását, akár felborulást is eredményezhet. Amennyiben nem jön jel egy adott kerékről, akkor a rendszer logikai vezérlése állónak feltételezi (ha a többi például mozgást mutat) és feltehetően megpróbál beavatkozni.

Az előfordulás (O) érzékenységvizsgálatát mutatja a 6.3. ábra, amely tanulságos eredményről számol be. Ez az egy kiugró eset (3-as számú) a legkritikusabb esemény előfordulásának magas voltára hívja fel a figyelmet, tehát célszerű lenne javítani a hiba

mérését, bekövetkezésének esélyét. Ránézésre a táblázatból nem szembetűnő, mivel nem kap magasabb vagy eltérő pontszámot a többi elemnél, viszont a grafikon jól mutatja fontosságát.

Végül az észlelhetőség (D) fejlesztésére hívja fel a figyelmet a 6.4. ábra, ismételten a kerék blokkolás észlelhetőségének javítására. Az észlelhetőség javításával szintén célszerű a biztonság (safety) oldalról is dokumentálni, hogy egy ilyen kiemelkedő hibát hogyan lehet megfelelően kezelni.

Az új értelmezés bevezetésével az RPN számhoz viszonyított érzékenységi együtthatókat mutatja a 6.5 ábra. A szembetűnő eltérést az első, a negyedik és az ötödik elem eltérő értelmezése jelenti. E három közül, jelen esetben az RPN szerinti rendezést tekintve az első számú a legsúlyosabb eset, míg az érzékenységvizsgálat az ötödik, hatodik eseteket előbbre sorolta. A példa esetében megfontolandó a vizsgálat eredménye, hiszen blokkoló kerékről érkező téves állapot adat következménye lehet ugyanúgy, mint egy hibás sebességi adat. A hibás blokkolási állapotnál nyilvánvalóbb a szenzor hibája, de a ráépülő funkcióknak rendelkezniük kell olyan hibakezelési lehetőségről, hogy ezt érzékeljék. A hibás abroncs sebességérték továbbítása megfontolandó hiba, amelyre szintén fel kell készíteni a rendszert.



6.5. ábra RPN, Ks_i, Ko_i, Kd_i ábrázolása egy koordináta rendszerben

6.2 Az érzékenységi együttható meghatározása hierarchikus Hibamód és –Hatáselemzésre

Az előző fejezetben ismertetett hibamód és -hatás analízist (FMEA) terjesztem ki a már ismertetett hierarchikus FMEA módszerével. Az elemzést az ismertetett kerékszenzoros rendszeren mutatom be, majd elvégzem az érzékenységvizsgálatot erre az FMEA-ra is. A példából felépített modell két teljes kiértékelésű szintből (rendszer és design), valamint két részben kiértékelt szintből (hatás és ok) szint áll. A VDA katalógus alapján „Product FMEA" azaz termék FMEA-nál ajánlott formanyomtatvány kerül alkalmazásra az elemzéshez. A hierarchia legfelső szintjén levő elemzés Effect Level (EL), azaz „hatás" szintnek tekintendő, amelyet a 6.5. táblázat mutat. Mint említésre került, ez a szint nem tartalmaz teljesen kiértékelt kockázatot, csupán a potenciális hibákat, azok hatásait és a súlyossági számokat.

No	Funkció	Pot. hiba	Pot. hiba hatása	*S*	Hiba oka	*O*	Prev./ Det. Akció	*D*	*RPN*
EL1	Meghatároz-ni az abroncs sebességét	Nem továbbít jelet	Sebesség nem meghatároz-ható	10	Nem továbbít jelet				
EL2			Rossz sebesség érték	7	Periodikus jel eltér az abroncs sebességé-től				
EL3	Észlelni a kerék-blokkolást	Blook-koló kereket nem érzékeli	Jármű instabillá válik	9	Kerék állapota gurulónak észlelve álló helyett				
EL4		Álló abroncs észlelve forgó abroncs helyett	Rossz információ a blokkoló kerék állapotáról	8	Blokkoló kerék nem detektált				
EL5				8	Kerék állapota állónak észlelve guruló helyett				

6.5. táblázat Hatás szint (Effect Level)

A hibák hatásához tartozó okokat egy szinttel lentebb, a rendszer szinten (System Level - SL) kerülnek származtatásra, míg a rendszerszinten levő funkciók meghibásodása és a hozzá tartozó súlyossági szám a hatás szintről (EL) kerül származtatásra. Ezzel biztosítva a rendszerben elemezendő hibák azonos jelentését és áttekinthetőségét. A jobb áttekintéshez célszerű a következő szintet is megismerni, amely a rendszer szint (System Level – SL). A hibahatásoknak rendszerszinten és az egész FMEA-ban jól követhetőnek és ugyanazon jelentést hordozónak kell lenniük. Ezt a követhetőséget logikai linkeléssel (összekapcsolással) célszerű megoldani, amelyet általában az FMEA készítő szoftverek támogatnak is. Az így létrejövő SL szintet a 6.6. táblázat mutatja, míg a szinteken át összekapcsolódó, végigvezetett hiba, ebben az esetben a „sebesség nem meghatározható" elem a 6.6 ábrán látható. Ez a módszer biztosítja az azonos jelentéstartalmat mind a súlyosság értékelésben (S) és értelmezésében egy-egy hibához tartozó minden elemzési szinten. Tehát a legmagasabb súlyosságú hiba mindvégig azonos súlyosságú marad.

No	Funkció	Pot. hiba	Pot. hiba hatása	S	Hiba oka	O	Prev./ Det. Akció	D	RPN
SL1	Periodikus jel előállítása a kerék forgása alapján	Periodi-kus jel eltér a kerék sebességtől	Rossz sebességi érték	7	A jeladó folyamatosan fémet érzékel	4	D: Ellenőrizni a kábel köteget P: Vízálló technológia használata	2	56
SL2			Rossz sebességi érték	7	Fogaskerék fogai között nem egyenletes a távolság	2	D Ellenőrzés egy másik szenzorral P: Előírni időszaki ellenőrzést a fogaskerékre	3	42
SL3		Nem továbbít jelet	Sebesség nem meghatározha tó	10	A jeladó nem érzékel fémeket	3	D: ellenőrizni az értékek hitelességét P: Meggyőződni a szenzor megfelelő rögzítéséről	3	90

SL4		Kerék blokkolása nincs észlelve	Hibás érték a blokkoló kerék állapotáról	8	Fogaskerék fogai között nem egyenletes a távolság	2	D: Gyártási audit P: Meggyőződni EoL méréssel	2	32
SL5	Periodikus jel frekvenciájának változtatása a kerék sebessége alapján	A kerék állapotát állónak érzékeli guruló állapot helyett	Hibás érték a blokkoló kerék állapotáról	8	A jeladó nem érzékel fémeket	2	D: Ellenőrizze a gyújtást is P: Ellenőrzés egy másik kerékkel	3	48
SL6					A jeladó folyamatosan fémet érzékel	2	D: Aperiodikus jel felismerése P: Meggyőződni a szenzor megfelelő rögzítéséről	3	48
SL7		A kerék állapotát gurulónak érzékeli álló állapot helyett	Jármű instabillá válik	9	Folyamatosan fém jelenlétét mutatja a szenzor	1	D: Összehasonlítás egy másik kerék állapotával P: Meggyőződni a szenzor megfelelő rögzítéséről	2	18

6.6. táblázat Rendszerszint (System Level)

A következő a tervezési szint (DL), ahol a fogaskerék, illetve az induktív szenzor kerül kiértékelésre (6.7. táblázat), a legalsó szinten pedig az okok (cause level - CL) kerülnek összegyűjtésre (6.8. táblázat), hasonlóan a legfelső hatás (effect - EL) szinthez.

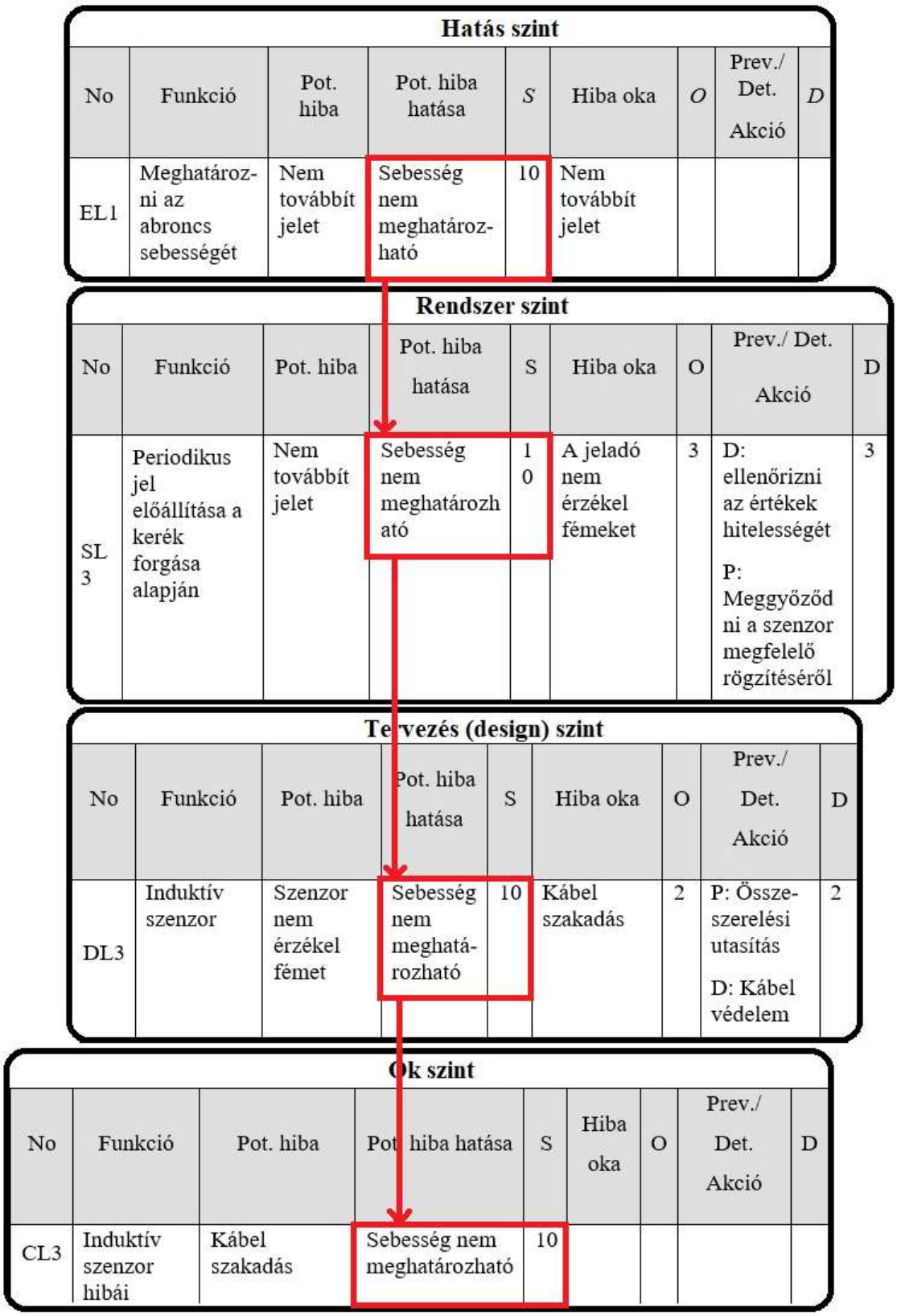
No	Funkció	Pot. hiba	Pot. hiba hatása	S	Hiba oka	O	Prev./ Det. Akció	D	RPN
DL1	Fogaskerék	Fogak közötti rés nem egyenletes	Rossz érték a blokkoló kerékről	8	Szennye-ződés a felületen vagy a fogak között	2	P: Össze-szerelési utasítás előírás D: Többi abroncs-al ellenőrizni a mérést	3	48
DL2		A fogak közötti rés nem megfelelő	Rossz érték a blokkoló kerékről	8	Túlságosan széles rés a fogak között	1	P: Gyártás utasítása ellenőr-zésre D: Termék mérése	2	16
DL3	Induktív szenzor	Szenzor nem érzékel fémet	Sebesség nem meghatá-rozható	10	Kábel szakadás	2	P: Össze-szerelési utasítás D: Kábel védelem	2	40
DL4		Szenzor folyama-tosan fémet érzékel	Sebesség nem meghatá-rozható	10	Kábel rövidzárban	2	P: Össze-szerelési utasítás D: Kábel védelem	2	40

6.7. táblázat A konstrukció szint (Design Level)

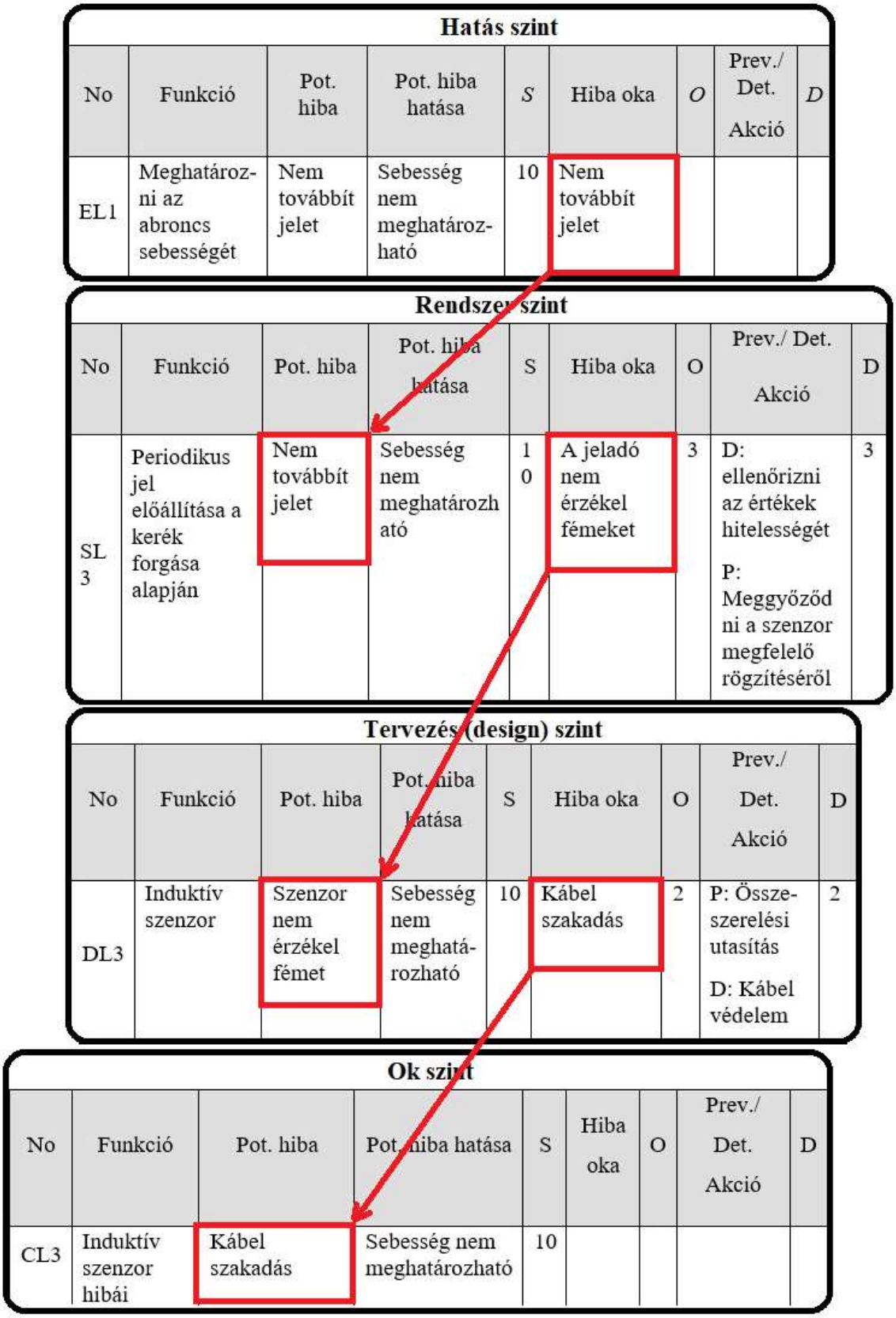
Korábban említésre került, hogy katalógusként is alkalmazható a CL szint, amelyet az adott szakterületnek specifikus ismert hibák összegyűjtésére is szolgálhat. Ezek ismeretében könnyebb lehet a fentebbi szintekre adott hibákat megtalálni, a rendelkezésre álló információkat felhasználva. Ezt az elvet a 6.7. ábra*6.7. ábra* mutatja.

No	Funkció	Pot. hiba	Pot. hiba hatása	S	Hiba oka	O	Prev./ Det. Akció	D
CL1	Fogaskerék hibái	Szennyeződés a fogazat felületén	Hibás érzékelés a blokkoló kerék állapotáról	8				
CL2		Túl széles fogköz	Hibás érzékelés a blokkoló kerék állapotáról	8				
CL3	Induktív szenzor hibái	Kábel szakadás	Sebesség nem meghatározható	10				
CL4		Kábel rövidzár	Sebesség nem meghatározható	10				

6.8. táblázat Az ok szint (Cause Level)



6.6. ábra A fentről lefelé (Top-down) származtatott súlyossági érték és hibahatás az effect szintről



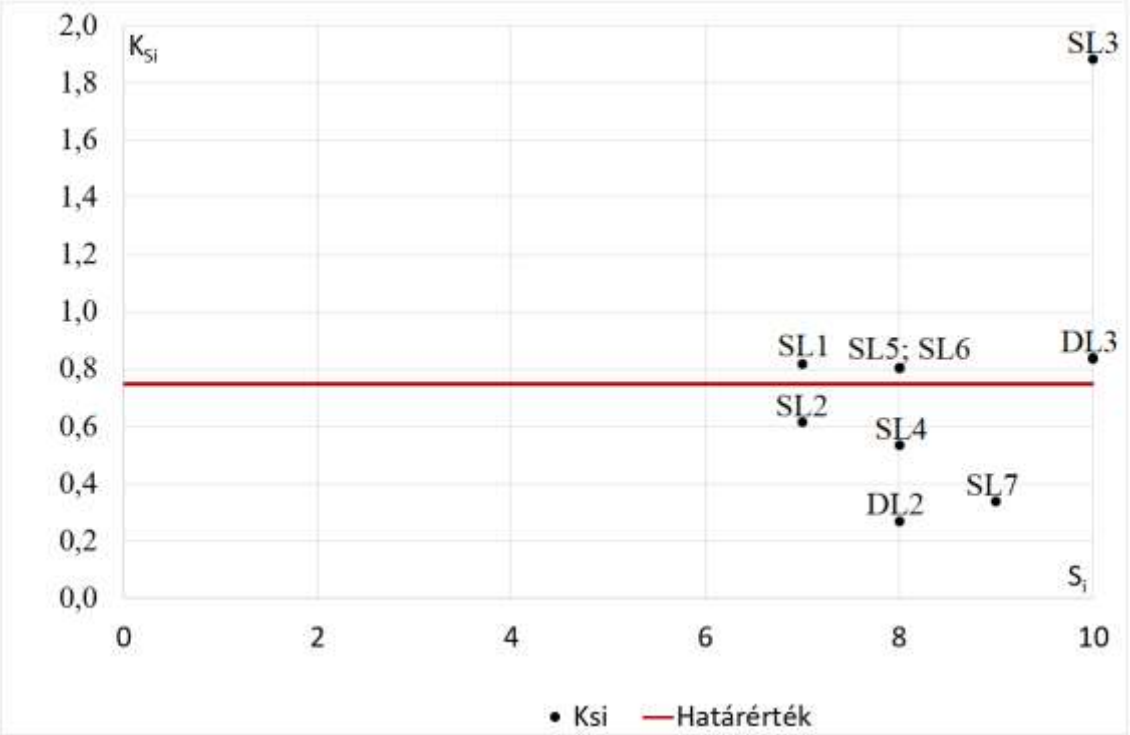
6.7. ábra Hibakatalógus az ok szintre (Cause Level)

A létrejövő efféle logikai kapcsolat biztosítja, hogy egy rendszer FMEA táblázataiban egy-egy hiba ugyanazon súlyossági értéket jelentse a táblázat egészében a már említett logikai kapcsolatokon keresztül. Az érzékenységvizsgálatot szintén elvégzem erre a hierarchikus elemzésre is. A számítások ugyanazzal a módszerrel történnek, mint az a hagyományos FMEA elemzés esetén. A kiszámított értékek a 6.9. táblázatban olvashatóak.

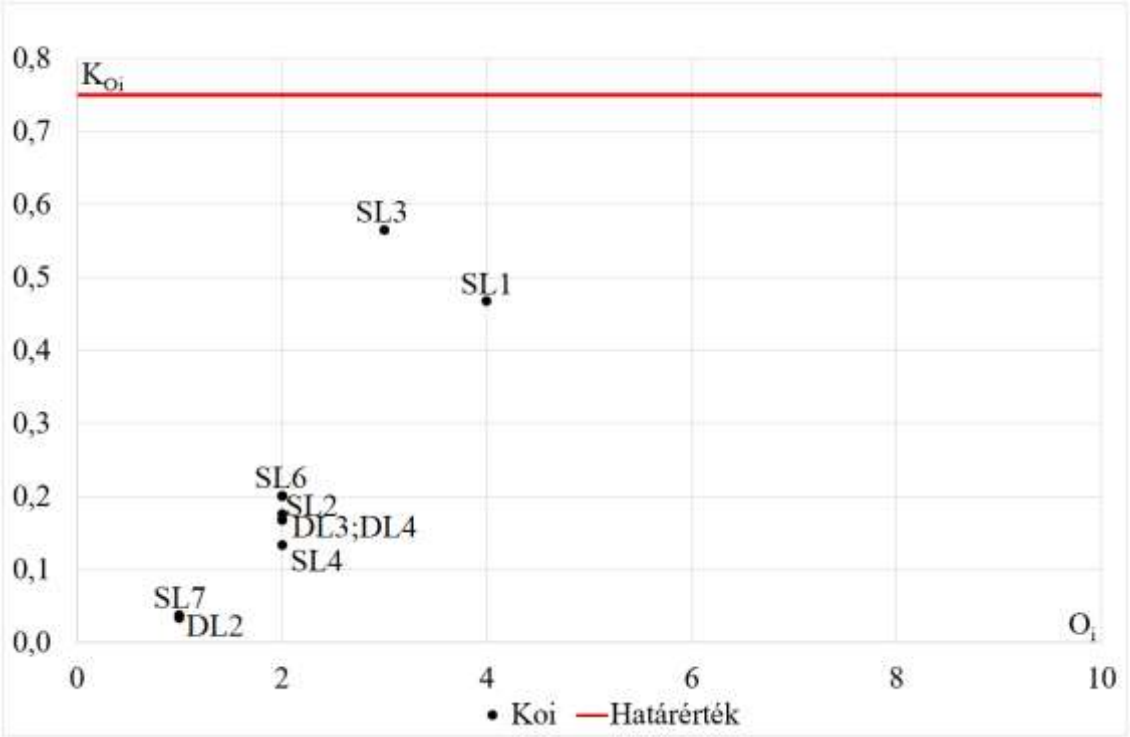
i	S_i	O_i	Di	RPN_i	K_i	K_{Si}	K_{Oi}	K_{Di}
SL1	7	4	2	56	0.1172	0.8201	0.4686	0.2343
SL2	7	2	3	42	0.0879	0.6151	0.1757	0.2636
SL3	10	3	3	90	0.1883	1.8828	0.5649	0.5649
SL4	8	2	2	32	0.0669	0.5356	0.1339	0.1339
SL5	8	2	3	48	0.1004	0.8033	0.2008	0.3013
SL6	8	2	3	48	0.1004	0.8033	0.2008	0.3013
SL7	9	1	2	18	0.0377	0.3389	0.0377	0.0753
DL1	8	2	3	48	0.1004	0.8033	0.2008	0.3013
DL2	8	1	2	16	0.0335	0.2678	0.0335	0.0669
DL3	10	2	2	40	0.0837	0.8368	0.1674	0.1674
DL4	10	2	2	40	0.0837	0.8368	0.1674	0.1674

6.9. táblázat A hierarchikus FMEA kockázati számok (RPN) és az érzékenységi értékek

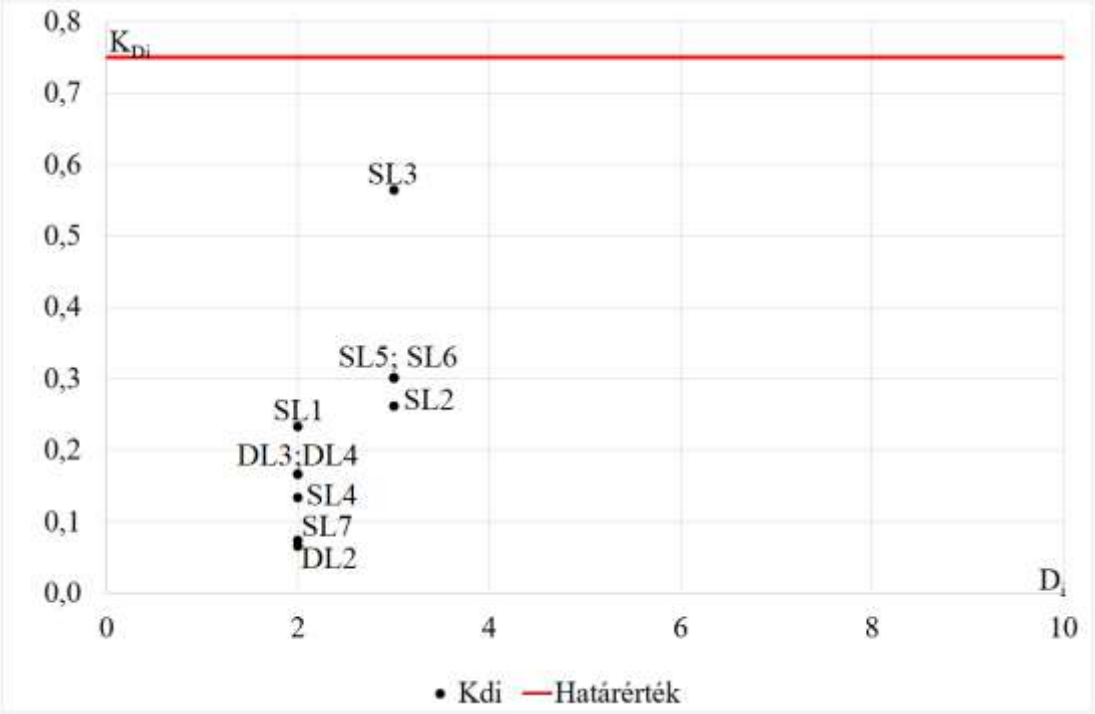
Az eredményeket grafikonon ábrázolva az alábbi grafikonok lesznek:



6.1. ábra Súlyosság érzékenységvizsgálata – hierarchikus modellezésnél

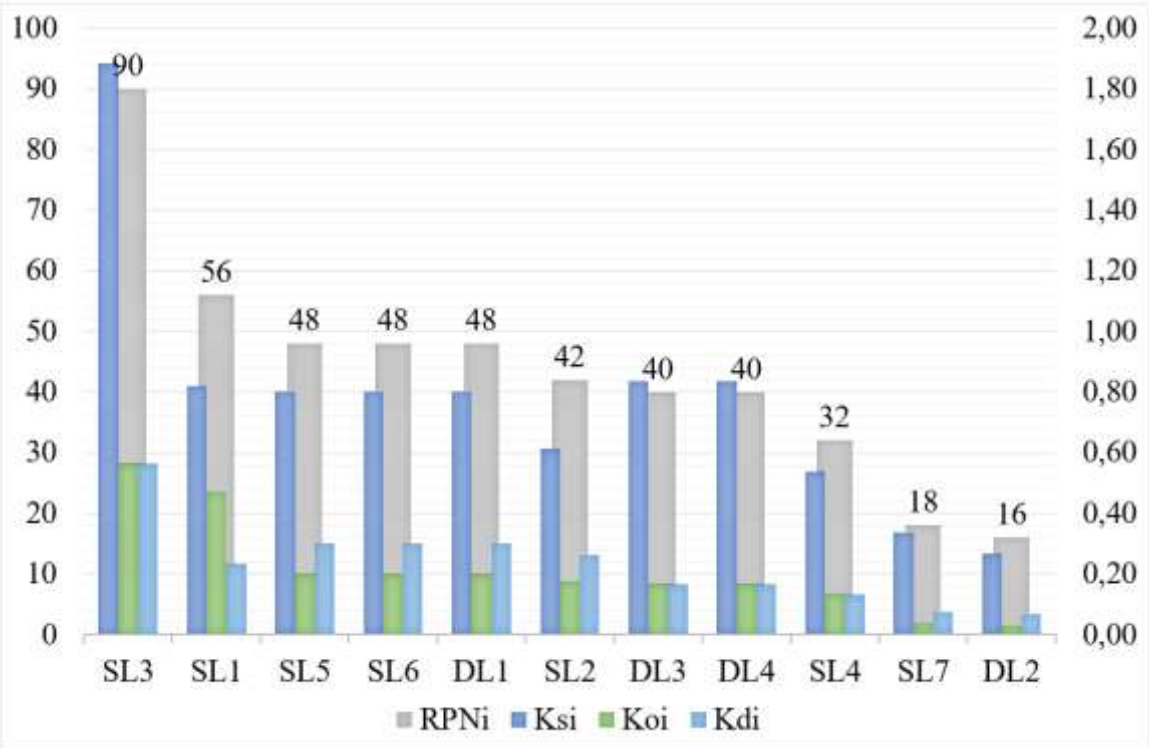


6.2. ábra Előfordulás érzékenységvizsgálata – hierarchikus modellezésnél



6.3. ábra Észlelhetőség érzékenységvizsgálata – hierarchikus modellezésnél

A most bemutatott, rendszer egészéhez viszonyított kockázat kiértékelési módszert a jelenleg használatos RPN számon alapuló kiértékeléshez összehasonlítva szintén eltérés figyelhető meg. Ezt mutatja a 6.12 ábrá*6.4. ábra*n is.



6.4. ábra RPN, Ksi, Koi, Kdi ábrázolása egy koordináta rendszerben – hierarchikus FMEA

Látható, hogy a szakma által is felismert probléma, amely már említésre is került, hogy az RPN érték nem reprezentálja teljesen a kockázat valódi tartalmát – itt is jól megfigyelhető. A grafikonon jól látható, hogyha az RPN alapján helyeznénk sorrendbe a kockázatokat, akkor SL3, SL1, SL5, SL6, DL1, SL2, DL3, DL4, SL4, SL7 és DL2. Ezzel szemben, a 6.12. ábrán az SL3 helye nem változott, de a DL3, DL4 jobban előtérbe került – az induktív szenzor üzemképtelenné válása, de változatlanul első helyen van mind a két esetben a nem meghatározható sebességből eredő hiba (SL3). Elvonatkoztatva az alkalmazástól – ez részben egy vezető halálos ok is az utakon, a nem megfelelő sebesség megválasztása. Azonban, ha egy járműrendszer esetén, csak erre a funkcióra épülne egy féket vezérlő rendszer (például: ESP- Electronic Stability Program), amely a kerekek szögsebességéből számítva törekszik a jármű alul- vagy felül kormányozottságát is kompenzálni – máris okozhatna kritikus helyzetet.

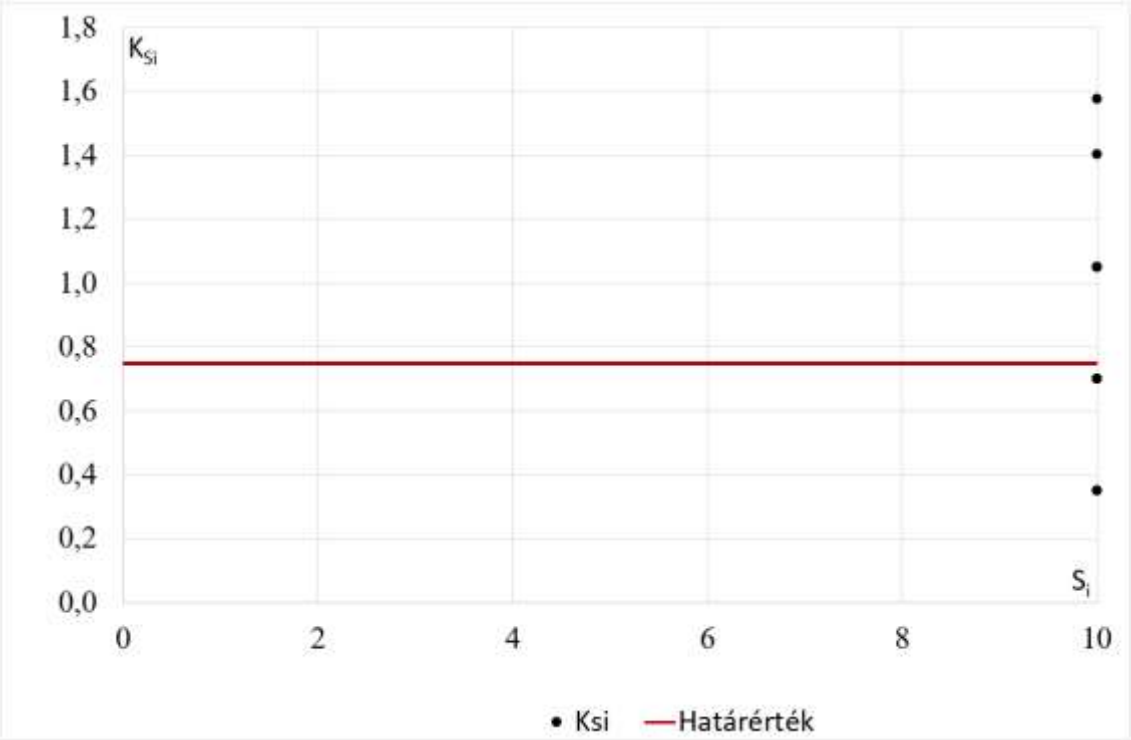
A bemutatott rangsorolási módszer feltehetően segíti a rendszermérnökök munkáját és a teszt menedzsereket a munkacsomagok tervezésében – rangsorolásában. A kritikus rendszerelemek kiemelése megkönnyebbülhet a grafikus reprezentáció segítségével és könnyebben prezentálhatóvá válik egy esetleges bemutatóra. [57]

A két elemzési módszerben annyi látszik, hogy a hierarchikus FMEA elemzésben bemutatott több szintű elemzéssel csak a súlyossági vizsgálatban mutatkoztak elemzendő eltérések. Ennek oka lehet az is, hogy a további elemzéssel a hibák jobban feltártak, és ha az alacsonyabb szinten derül fény hiányosságra – jobban tudnak célzottan reagálni. Esetünkben a kockázati szám (RPN) növekedésével kicsit differenciálódott ugyan az FMEA, de lényegi nagy változást nem hozott. Véleményem szerint egy jelentősen nagyobb adatbázisban nyújthat segítséget, ahol sokkal nehezebbé válik az áttekinthetőség a puszta táblából kiolvasható értékek tanulmányozásával.

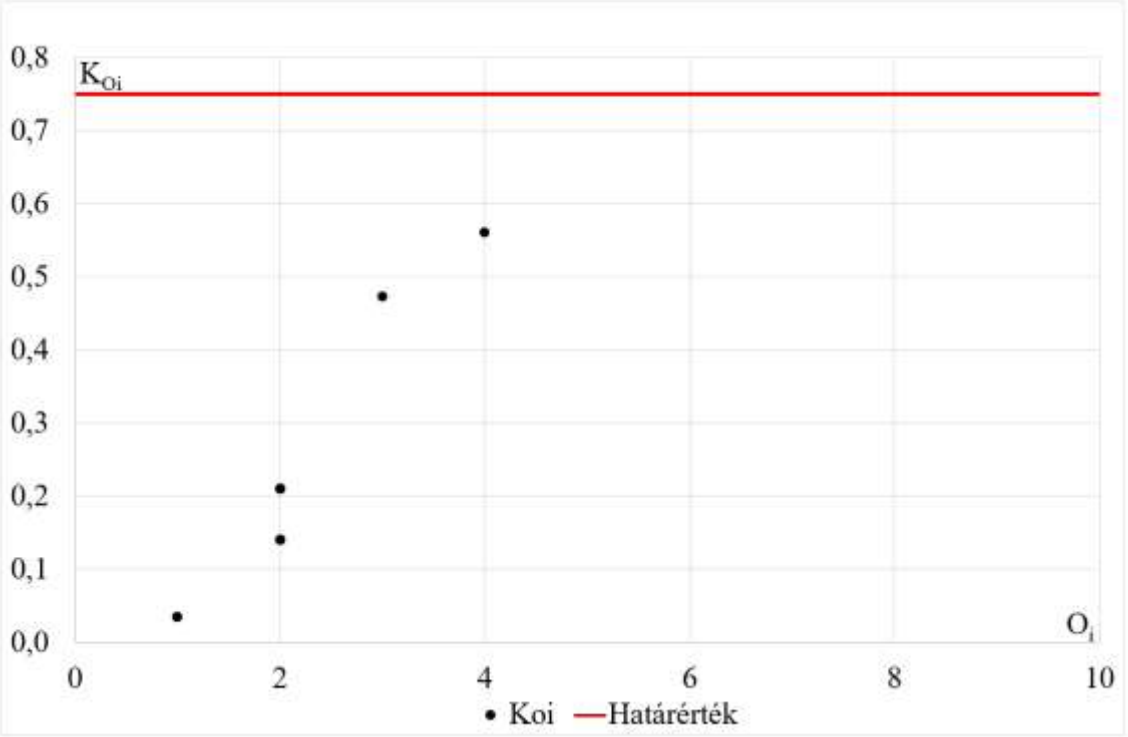
6.3 Következtetések, ajánlások

A fejezetben bemutatásra került a hierarchikus és az elterjedtebb hagyományos, egyszintű FMEA érzékenységvizsgálata. Látható, hogy a keréksebességmérő szenzor mélyebb analízisével finomodnak a kockázati tényezők az elvárásnak megfelelően. De nem szabad elfeledkezni a kockázatértékelés finomításának igényéről sem, amellyel mélyebb áttekintés kapható a rendszer egészét veszélyeztető elemi okokról a rendszer egészéhez viszonyítva. A grafikus reprezentáció növeli az átláthatóságot és az elemzés szakterületében kevésbé jártas szakemberek számára ad értelmezhető formátumot.

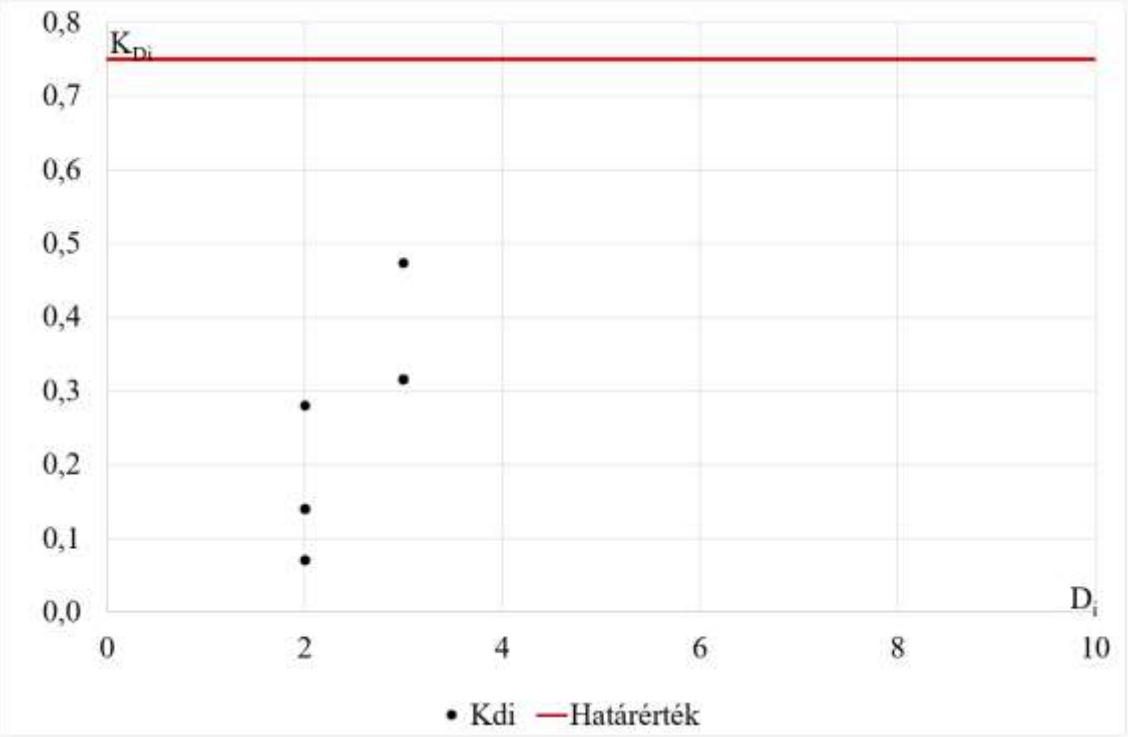
A tapasztalati úton megállapított határérték jól elkülöníti és szemlélteti a vizsgálandó funkciók működési biztonságának szintjét. Ez alatt arra gondolok, hogy mennyire akadályozzák meg annak meghibásodását, és ha hibásan működik, akkor mennyire könnyen veszik azt észre. Az érzékenység vizsgálat az FMEA esetében segít megtalálni egyrészről azt a hibát, amely ellen leginkább védekezni szükséges, illetve a súlyossági térképen nagyságrendi információ kapható mindezekről és segít a „hogyan védekezzünk?" kérdésben is elindulni. Tegyük fel, hogy az előző fejezetekben bemutatott kerékszenzoros rendszerükben minden súlyossági (S) érték maximálisra változik (S=10) és a többi érték változatlan marad. Erre átrendeződő grafikon látható a 6.13-6.15 ábrákon.



6.5. ábra Maximális súlyossági (S) értékek esetén a
H-FMEA – súlyossági érzékenység



6.6. ábra Maximális előfordulási (O) értékek esetén a
H-FMEA – előfordulási érzékenység



6.7. ábra Maximális észlelhetőségi (D) értékek esetén
a H-FMEA észlelési érzékenység

Látható, az összes érték a határérték vonal felett lehetne ugyan, de a számítás figyelembe veszi az észlelhetőség és előfordulás súlyát is az elemzett rendszerben. Ezért jobban differenciálódik a veszélyt jelentő elemek ábrázolása a súlyosság- és előfordulás terén. Az észlelhetőség nem változik szembetűnően ez esetben.

7 ÖSSZEFOGLALÁS

Disszertációmban a gépjárműipar fejlesztési szakaszában kötelezően elvégzendő hibamód és -hatáselemzés (FMEA) általam is megtapasztalt alkalmazási és modellezési problémájára dolgoztam ki megoldást. Személyesen tapasztaltam meg, hogy az egyre összetettebb és bonyolultabb járműirányítási rendszereket nagyon változatos minőségű modelleken keresztül elemzik. Nagyon nagy szó, ha egy közös szemléletmódot tud bevezetni a vállalat, amelyet a legtöbb szakember elfogad. Az analízis készítését moderáló munkatárs sokszor egy adminisztratív feladat elvégzésének és favágásnak érzi feladatát, nem törekszik egységesítésre és eredmények elérésére az előzetes kockázatelemzés elkészítésében. Az ilyen hozzáállás eredménye, hogy egy szükséges rosszként tekintenek az FMEA-ra, mert lényegi eredményt nem kapnak belőle és nem látható egy fejlesztő számára az eredmény, amely az ő közvetlen munkájához hasznos visszajelzéseket adhatna. Az elemzést azonban, mint említésre került - a minőségirányítási rendszer és az iparági „state of the art" szabványok követelik meg. A bemutatott hierarchikus elrendezést elsősorban a funkcionális biztonsági szabvány írja elő, de módszeri alkalmazást vagy „best practice"-t nem ismertet.

A járműrendszerek egységesített modellezését korábbi tapasztalataim alapján dolgoztam ki, amelyet a megbeszélések alkalmával is sikeresen alkalmaztam. Az eredmények egyrészről követhetőséget adtak a gyártás számára, illetve csökkentették a készítési időt és olyan logikai kapcsolatok létrejöttét tették lehetővé, amellyel egyértelműen azonosíthatóvá vált egy-egy elem kapcsolódási pontja a rendszermodellben is. Ilyen lehetett például az ESP mint szoftvermodul helyének a meghatározása, hiszen egy jármű egészére van hatással, kapcsolatban áll a fékrendszer valamennyi elemével (utasítást ad és értékeket olvas be), gyártóskor átadott konfigurációs paraméterek alapján működik és közvetlenül dolgoz fel szenzorról érkező jeleket, de mégis egy szoftver komponens fizikailag. Az elemzés eredményeként világosan kiderült, hogy ez a modul a járműrendszer alatt közvetlenül helyet foglaló funkció, amelyhez célszerű közvetlenül kapcsolni legyező- és kormányszög mérő szenzorokat. Ez a felismerés a funkcióbiztonsági elemzésekben nyújtott segítséget a Safety csoport számára is.

Azonban a magasabb szintű biztonsági kockázatok elemzésénél megfogalmazódott a hibák létrejöttének mélyebb megismerési igénye. Erre a hibafa elemzést írják elő, magasabb szintű biztonsági besorolásnál (ASIL C, ASIL D), így egyenesen kötelezve is vannak a

fejlesztést végzők. A hibafa eredményeinek értelmezésében az egyik legfontosabb megtalálni azokat az elemi hibákat, amelyek közvetlenül vagy más elemi hibával együttesen veszélyeztetik a rendszert. Ehhez került alkalmazásra az érzékenységi vizsgálaton alapuló LFTSM módszer. Nagy előnye, hogy könnyen algoritmizálható, és mint számszerű úgy grafikus reprezentáló eredményeket nyújt. A szoftverkomponensek fejlesztési minőségének javítása is megfogalmazódott, amelyet a tesztek mellett robusztus fejlesztési folyamattal biztosítanak. A gyenge pontok megtalálása azonban nem triviális egy minőségirányítási mérnök számáram ezért a kérdést megfordítva a fejlesztésből kiindulva került felmérésre a szoftverfejlesztési folyamat sérülékenysége. Pontosabban feltételezve, hogy egy hibát az adott folyamat betartásával lehet megelőzni. Az adódó hibát és előfordulást alapul véve került vizsgálat alá a fejlesztési folyamat érzékenységi vizsgálata.

A hibafa eredményeit tovább gondolva az FMEA érzékenységvizsgálata is felvetődött. Szembetűnő, hogy a kockázati szám a szorzás művelete miatt eltérő tartalmú lehet. Ezt a problémát maga a VDA is felismerte és elkezdtek mátrixok alapú térképekben gondolkodni, amely nem hozott egységes megoldást. A dolgozatban bemutatott érzékenységi együttható vizsgálati módszerével azonban a rendszer egészéhez viszonyítva kerül egy-egy elem esetlegesen kiemelésre. A grafikus reprezentációt a jobb szemléltetés mellett az összehasonlíthatóság- és áttekinthetőség növelése miatt tartottam fontosnak bevezetni. A rendszerek vizsgálatában kirajzolódott, hogy a hierarchikus elrendezés tovább pontosítja az eredményeket az egyszintű, hagyományos elrendezésnél. A létrejött viszonyítási értékek segítségével az RPN kockázati szám mellett az egyes tényezők jelentős kiemelkedése jobban elkülönül. A tervezők könnyebben tudnak mérlegelni az adott kockázat kezelési stratégiájáról és hatásosabb intézkedéseket tudnak ezáltal megfogalmazni és bevezetni.

7.1 Új tudományos eredmények

Az értekezésemben bemutatott kutatómunka új tudományos eredményei az alábbi tézisekben foglalható össze:

1. Kidolgoztam a Hibamód- és Hatás Elemzés (FMEA) érzékenységi vizsgálatának egy új módszerét.

   1.a Bevezettem a $K_{S_i}, K_{O_i}, K_{D_i}$ funkcionális érzékenységi együtthatók fogalmát.

   1.b Grafikus ábrázolási módszert dolgoztam ki, mely az elemzett rendszer összkockázati értékéhez viszonyítva áttekintést adn az elemek kockázati tényezőinek a rendszer megbízhatóságára gyakorolt hatásaira a bevezetett funkcionális érzékenységi együtthatók, illetve a súlyosság (S), előfordulás (O) és észlelhetőség (D) paraméterek függvényében.

   1.c Bizonyítottam, hogy az általam bevezetett funkcionális érzékenységi együtthatók alkalmazásakor azonos értékű RPN kockázati számmal bíró elemek kockázati határainak differenciálási lehetősége biztosítható.

   1.d A Lineáris Hibafa Érzékenységi Modell (LFTSM) elemzés eredményeivel összehasonlítva igazoltam, hogy az általam kidolgozott elemzés áttekinthetőbb képet ad a vizsgálandó rendszer megbízhatóságának gyenge pontjairól.
   Kapcsolódó publikációim: [96], [97], [98], [99], [100]

2. Haapannen szoftver komponensek funkcionális Hibamód és –hatáselemzés modelljében definiált „system kernel” szintje és „application software” szintek közé egy „kommunikációs interfész” szintet vezettem be. Új, három, egymásra épülő logikai szintű FMEA modellt definiáltam.
   Kapcsolódó publikációm: [95]

3. Kidolgoztam a Hierarchikus Hibamód- és Hatáselemzés (H-FMEA) egy új, egységes modellezési módszerét.

   3.a Az elektronikus hardver, szoftver és mechanikai komponensek funkcióinak kockázat elemzését egy közös, átfogó rendszerbe foglaltam össze.

3.b A mechanikai alkatrészeket a termék működésében betöltött funkciójuk alapján csoportokba rendeztem. A csoportokat felsőbb szinten, Rendszer FMEA-kban, míg a funkciót megvalósító alkatrészeket Konstrukciós FMEA-kban az alsóbb szinten helyeztem el, a két szint közötti hierarchikus logikai kapcsolatot leírva.

3.c Továbbfejlesztettem a gyártási minőségbiztosítás speciális karakterisztikáinak rögzítését az alkatrészeket csoportosító funkcióhoz rendeltem, hogy egyértelműen azonosítható legyen az adott karakterisztika létrehozásának indoka, illetve egy esetleges változtatást követően is látható maradhasson a karakterisztika létrehozásának alapja.

3.d A meghibásodások okait tovább vezettem az elemzés ok (cause) szintjére, hogy az előforduló hibák okairól egy gyűjtemény készüljön. Így a későbbi elemzések fel tudják használni a korábban azonosított hibaokokat.

Kapcsolódó publikációm: [95]

7.2 Ajánlások

Értekezésemben bemutatott kutatási munka új tudományos eredményeinek hasznosítási lehetőségeit az alábbiakban foglalom össze:

1. A H-FMEA sablon kidolgozásával a Funkcionális Biztonsági Szabvány (ISO 26262) által is előírt hierarchikus elemzés kötelező alkalmazását könnyítem meg egy átlátható, mind a három diszciplína összekapcsolására alkalmas háttérrel.

2. A komplex szoftverkomponensek modellezésénél nehezen látható át, hogy a számos függvény közül mit emeljünk ki funkciónak az elemzéshez, illetve ezek hogyan kapcsolódjanak össze. Létezik ugyan szoftver architektúra tervezés, modellezési szabvány (AUTOSAR) és modellezési nyelv (UML), de az átláthatóságot és a lényegi funkciók kiemelését, valamint logikai kapcsolását növeli az általam kialakított három csoportosítási szint és értekezlet-vezetési stratégia.

3. A mechanikai rendszerek áttekinthetőségét növeli, ha nem csupán az alkatrészekre és azok fizikai paramétereire koncentrálunk kiértékelés készítésekor, hanem a termékben betöltött funkciójára is. Hasznosabb, ha a termék tervezési szempontjait igyekezünk kiértékelni és nem a tervezőjének a munkáját. Ez által egységessé vált elemzésben egy ellenőrzési listát alkalmazva – gyorsul a kiértékelés. A speciális karakterisztika jelölésére kidolgozott módszeremmel a gyártás számára is követhetővé válik az egyes változtatások okának kiderítése.

4. A katalógus jellegű ok (cause) szint kidolgozásával a létrejövő katalógusok jó kiindulási alapot nyújtanak egy-egy tervezői (design) FMEA hiba okainak megállapításához. A korábbi FMEA-kból gyűjtött hibaokok jó gondolatébresztőként szolgálnak a megbeszéléseken, felgyorsítva az egyes jellemző hibaokok megfelelő szintű megfogalmazását.

5. A kockázati számok kiértékelésének egy új, grafikus reprezentálási módja támogatást nyújt az auditok és a menedzseri jelentések összehasonlíthatóságának elősegítésébe. A feldolgozás automatizálható, így hónapról-hónapra követhető az adott rendszer S, O, D paramétereinek eloszlása, illetve a rendszerben azonosított kockázatok súlyosságának méretére és mennyiségére is.

8 IRODALOMJEGYZÉK

8.1 Felhasznált irodalom

[1] Abonyi J., Fülep T.: Biztonságkritikus rendszerek, Elektronikus jegyzet, Pannon Egyetem, 2014 http://moodle.autolab.uni-pannon.hu/Mecha_tananyag/biztonsagkritikus_rendszerek/index.html (Letöltve: 2018.04.07)

[2] A hibafa története, https://en.wikipedia.org/wiki/Fault_tree_analysis#History (Letöltve: 2018.04.07)

[3] A V-modell, http://appdevcare.hu/wp-content/uploads/2014/11/img21.png (Letöltve: 2018.04.07)

[4] AIAG bemutatása, https://www.aiag.org/about 2015 (Letöltve: 2018.04.07)

[5] Analysis Techniques For System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA), Geneva: International Electrotechnical Commission, 2006.

[6] APQP rövid bemutatása, http://www.mibi.hu/doc/APQP.pdf 2015 (Letöltve: 2018.04.07)

[7] Barbara J. Youngberg, Martin J. Hatlie: The Patient Safety Handbook, Jones & Bartlett Learning, ISBN:0-7637-3147-1, 2004 pp 131-134

[8] Bulander R.: Electrification is taking combustion engines to new heights, Robert Bosch GmbH, presentation in Boxberg, https://www.bosch-presse.de/pressportal/de/media/migrated_download/Electrified_slides.pdf, 2015 (Letöltve: 2018.04.07)

[9] Choi J.: NADA UCG's 2014 Car Shopper Survey Ranks Consumer Preferences for New Vehicles, Car & Truck Blog, 2014 http://www.nada.com/b2b/NADAOutlook/UsedCarTruckBlog/tabid/96/entryid/482/nada-ucg-s-2014-car-shopper-survey-ranks-consumer-preferences-for-new-vehicles.aspx (Letöltve:2018. 04.07)

[10] Chotaliya J.: Connected Car, Internet of Things Mumbai Meetup (IoTMUM), 2014. https://www.slideshare.net/spukale/connected-cars-iotmum-org (Letöltve:2018. 04.07)

[11] Clemens P. L.: Fault tree analysis, 4th edition, Sverdup, 1993 http://s3.spanglefish.com/s/22631/documents/safety-documents/fta-tutorial.pdf (Letöltve: 2018.04.07)

[12] Collett R. E., Bachant P. W.: Integration of BIT Effectiveness with FMECA, 1984 Proceedings of the Annual Reliability and Maintainability Symposium, NY: New York, IEEE, 1984

[13] Dabboussi A., Kouta R., Gaber J., Wack M., Hassan B. E. and Nachabeh L., "Fault tree analysis for the intelligent vehicular networks," 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM), Jounieh, 2018, pp. 1-6. doi: 10.1109/MENACOMM.2018.8371027

[14] Daróczi M.: Projektmenedzsment, egyetemi jegyzet, Szent István Egyetem, 16. fejezet, https://www.tankonyvtar.hu/hu/tartalom/tamop412A/2010-0019_Projektmenedzsment/ch16.html 2014
(Letöltve: 2018.04.07)

[15] Deb S., Ghoshal S., Mathur A., Shrestha R., and Pattipati K. R., "Multi-signal modeling for diagnosis, FMECA, and reliability," Proceedings of the 1998 IEEE International Conference on Systems, Man, and Cybernetics, San Diego, October 11-14, 1998. pp. 3-17

[16] Definition APQP – Was ist APQP?
http://quality.kenline.de/seiten_d/apqp_definition.htm
(Letöltve: 2018.04.07)

[17] Deloitte: Global Automotive Consumer Study, Exploring consumers' mobility choices and transportation decisions, 2014.
https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-auto-global-automotive-consumer-study-100914.pdf
(Letöltve:2018. 04.07)

[18] „Design Failure Mode and Effect Analysis" Reference edition, ISBN:978-1-60534-136-1, 2008 – 18-21.oldal

[19] Desjardins J.:How many millions of lines of code does it take?, 2017,
http://www.visualcapitalist.com/millions-lines-of-code/
(Letöltve:2018. 04.07)

[20] Die häufigsten Pannenursachen 2014, ADAC,
http://www.auto.de/magazin/customs/uploads/auto/2015/02/ADAC-Pannenhilfea-93416.jpg
(Letöltve:2018. 04.07)

[21] Die Häufigsten Ursachen von LKW, ADAC
http://www.reisenews-online.de/pics/ursachen-von-lkw-pannen-2011/
(Letöltve:2018. 04.07)

[22] DIN EN ISO 9004, Quality management – Quality of an organization – Guide to achieve sustained success (ISO/DIS 9004:2017)

[23] Euroean Commission, Mobility and transport, Road safety, Statistics – accidents data, Road fatalities in the EU since 2011 (graph)
https://ec.europa.eu/transport/road_safety/sites/roadsafety/files/move-affiche-hoz_en_2017_debord.pdf
(Letöltve:2018. 04.07)

[24] Európai Parlament 2008/0100(COD) számú eljárása, 2008,
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A6-2008-0482+0+DOC+XML+V0//HU
(Letöltve:2019. 01.07)

[25] Failure Modes & Effects Analysis, University of Calgary (Canada), 2002. http://people.ucalgary.ca/~design/engg251/First%20Year%20Files/fmea.pdf (Letöltve: 2018.04.07)

[26] Faulconbridge R. I., Ryan M. J.: Managing Complex Technical Projects: A Systems Engineering Approach Artech House Boston, London, 2003 – Chapter 1. ISBN: 1-58053-378-7

[27] Ferber I.: FMEA: valami régi és valami új az egészségügyben, A termelési folyamat minőségkérdései vizsgálatok, BME Országos Műszaki Információs Központ és Könyvtár, 2005 http://www.omikk.bme.hu/collections/mgi_fulltext/minoseg/2005/12/1209.pdf (Letöltve: 2018.04.07)

[28] FMEA alkalmazására egy képernyőkép, http://www.plato.de/tl_files/public/EN/Produktportfolio/Importer/Importer.jpg (Letöltve: 2018.04.07)

[29] FMEA Handbook Version 4.2, Ford Motor Company, 2011 p19

[30] Goldberg B. E,, Everhart K., Stevans R., Babitt N. III, Clemens P. és Stout L.: System Engineering "Toolbox" for Design-Oriented Engineers, National Technical Information Service, NASA, 1994. https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19950012517.pdf (Letöltve: 2018.04.07)

[31] Haapanen P., Helminen A.: Failure Mode and effects analysis of software based automation systems, STUK-YTO-TR190, 2002, pp 21-23.

[32] Hecht H., Xuegao A. and Hecht M., "Computer aided software FMEA for unified modeling language based software," Annual Symposium Reliability and Maintainability, doi: 10.1109/RAMS.2004.1285455 2004 - RAMS, Los Angeles, CA, USA, 2004, pp. 243-248. (Letöltve: 2019.01.07)

[33] Hillenbrand M: Funktionale Sicherheit nach ISO 26262 in der Konzeptphase der Entwicklung von Elektrik/Elektronik Architekturen von Fahrzeugen, KIT Scientific Publishing, ISBN:978-3-86644-803-2, 2012

[34] Homkes R., Evenecky D., Kraebber H.: Applying FMEA to Software, Proceedings of the 2005 American Society for Engineering Education Annual Conference & Exposition, American Society for Engineering Education 2005

[35] Hughes N.,Chou E., Price C., Lee M.: Automating Mechanical FMEA Using Functional Models, Proceedings of the Twelfth International FLAIRS Conference, AAAI, 1999

[36] ISO 26262:2011, Road vehicles – Functional Safety, ISO standard, 2011.

[37] ISO/TS16949-es hivatkozásnál: Quality managemetn systems – Particular requirements for the appllication of ISO 9001:2008 for automotive production and relevant service part organizations (2009)

[38] Johanyák Cs. Zs.: Hibalehetőség és hibajavítás elemzés alkalmazása a szoftverfejlesztésben, ISBN 963 472 691 7, Debrecen, 2002.

[39] Kefferpütz R.:Car wars: The future of Europe's car industry, Green Eurpoean Journal, 2018, https://www.greeneuropeanjournal.eu/car-wars-the-future-of-europes-car-industry/
(Letöltve:2018. 04.07)

[40] Kellner W. D. – Software FMEA: A successful application for a complex service oriented archtecture system, IEEE 978-1-5090-5284-4/17/$31.00, 2017

[41] Kmenta S., Ishii K.: Advanced FMEA using meta behavior modeling for concurrent design of products and controls, in: Proceedings of the 1998 ASME Design Engineering Technical Conferences, 1998.

[42] Kocmanová A., Dočekalová M., Luňáček J. (2013) PROMETHEE-GAIA Method as a Support of the Decision-Making Process in Evaluating Technical Facilities. In: Hřebíček J., Schimak G., Kubásek M., Rizzoli A.E. (eds) Environmental Software Systems. Fostering Information Sharing. ISESS 2013. IFIP Advances in Information and Communication Technology, vol 413. Springer, Berlin, Heidelberg, Online ISBN 978-3-642-41151-9, 2013.

[43] Kumar A.: Overview of industrial risk assessment, The Regional Environmental Center for Central and Eastern Eurpoe, 2011.
http://web.iitd.ac.in/~arunku/files/CEL899_Y13/Industrial%20Risk%20Management_Overview.pdf
(Letöltve: 2018.04.07)

[44] Lake J.: Unraveling the Systems Engineering Lexicon, Proceedings of the INCOSE Symposium, 1996.

[45] Li S., Duo S.: Safety analysis of software requirements: model and process, 3rd International Symposium on Aircraft Airworthiness, ISAA 2013
https://ac.els-cdn.com/S1877705814011643/1-s2.0-S1877705814011643-main.pdf?_tid=db36bced-92d3-45aa-b650-bf825cb51498&acdnat=1531489991_552dc57821fa789617162ad7267909f3
DOI: 10.1016/j.proeng.2014.09.071
(Letöltve: 2018.07.13)

[46] Liu H.-C., Song W., Su Q., Li Z.: Failure Mode and Effect Analysis Using Cloud Model Theory and PROMETHEE Method, IEEE, 2017
DOI: 10.1109/TR.2017.2754642
(Letöltés: 2018.05.20)

[47] Macher G., Sporer H., Brenner E., Kreiner C. J.: Supporting Cyber-Security based on hardware-software interface definition, Springer 2016, DOI: 10.1007/978-3-319-44817-6_12
(Letöltés: 2018.05.20)

[48] Marshall J.: An Introduction to Failure Modes Effects and Criticality Analysis FME(C) A, The University of Warwick, 2011
http://www2.warwick.ac.uk/fac/sci/wmg/ftmsc/modules/modulelist/peuss/slides/section_10b_fmea_lecture_slides_compatibility_mode.pdf
(Letöltve: 2018.04.07)

[49] Martins E. F., LIMA G. B. A., SANT'ANNA A. P., FONSECA R. A. d., SILVA P. M. d., GAVIÃO L. O.: Stochastic Risk Analysis: Monte Carlo Simulation and FMEA (Failure Mode and Effect Analysis), Espacios, Vol. 38, No. 04, ISSN 0798 1015, 2017. pp 2

[50] Mészáros M.: Félvezető eszközök, áramköri elemek I. NSZFI, elektronikus jegyzet, p8 http://kepzesevolucioja.hu/dmdocuments/4ap/6_0917_011_101115.pdf (Letöltés: 2019.01.20)

[51] MIL-STD-1629A, MILITARY STANDARD: PROCEDURES FOR PERFORMING A FAILURE MODE, EFFECTS, AND CRITICALITY ANALYSIS (24 NOV 1980)

[52] MIL-STD-785B, MILITARY STANDARD: RELIABILITY PROGRAM FOR SYSTEMS AND EQUIPMENT DEVELOPMENT AND PRODUCTION (15 SEPT 1980)

[53] MSZ EN 60812:2006 „A rendszer-megbízhatóság elemzési módszerei. A hibamód- és hatáselemzés (FMEA) eljárása (IEC 60812:2006)"

[54] MSZ IEC 50(191):1992 Megbízhatóság és szolgáltatás minősége

[55] Murphy S., Schaeffers M.: The use of specification symbols, special characteristics and RPN rating, Datalyzer, 2017 https://datalyzer.com/wp-content/uploads/2017/03/FMEAclassification.pdf (Letöltve: 2018.04.07)

[56] NASA-GB-8719:13-2004. NASA Software Safety Guidebok, National Aeronautics and Space Administration, 2004 https://standards.nasa.gov/standard/nasa/nasa-gb-871913 (Letöltve: 2018.04.07)

[57] Nesic Z., Ljubic L., Radojicic M. and Vasovic J.V.: Analysis of the information flow within the information system of car parks, Acta Polytechnica Hungarica, vol 12, no. 3. 2015. pp. 73-86

[58] Paul A. E.:Most 2014 GM cars will also be a Wi-Fi hotspot, NBCnews, 2013.02.25 accessed 2018.12.04, https://www.nbcnews.com/businessmain/most-2014-gm-cars-will-also-be-wi-fi-hotspot-1C8539395 (Letöltve: 2019.01.07)

[59] Paul d. V., Lai X.: Resilience analysis of service-oriented collaboration process, Service Oriented Computing and Applications (2018) 12, pp25-39

[60] Pete T., Morris A., Talbot R., Fagerlind H.: Identifying the causes of road crashes in Europe, 57th AAAM Annual Conference, Annals of Advances in Automotive Medicine, September 22-25, 2013

[61] Plósz S., Schmittner C., Varga P. (2017) Combining Safety and Security Analysis for Industrial Collaborative Automation Systems. In: Tonetta S., Schoitsch E., Bitsch F. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2017. Lecture Notes in Computer Science, vol 10489. Springer, Cham

[62] Pokorádi L., Fülep T.: (2013) Reliability in Automotive Engineering by Fuzzy Rule-Based FMEA. In: SAE-China, FISITA (eds) Proceedings of the FISITA 2012 World Automotive Congress. Lecture Notes in Electrical Engineering, vol 197. Springer, Berlin, Heidelberg

[63] Pokorádi L.: Rendszerek és folyamatok modellezése, Campus Kiadó, Debrecen, ISBN:978-963-9822-06-1, 2008

[64] Pokorádi L.: Sensitivity Investigation of Fault tree analysis with Matrix-Algebraic Method, Theory and Applications of Mathematics & Computer Science vol.1, 34-44, 2011

[65] Pölöskeiné Hegedűs H.: Projektmenedzsment I., http://centroszet.hu/tananyag/projektmenedzsement, 2009, (Letöltve: 2018.04.07)

[66] C. Price and N. Snooke: An Automated Software FMEA, International System Safety Regional Conference, Singapore, April 2008

[67] QS9000: Quality System 9000, Quality System Requirements (QS 9000:1994)

[68] Quality Management in the Automobile Insdustry, Quality Assurance Prior to Serial Production, Product and Process FMEA, VDA (Verband der Automobilindustrie) volume 4, 2006

[69] Rupp C., Pohl K.: Requirements Engineering Fundamentals: A Study Guide for the Certified Professional for Requirements Engineering Exam - Foundation Level - IREB compliant, 2nd Edition, Rockynook, ISBN 978-1-937538-77-4, 2015

[70] Rising M. J., Levenson G. N.: Systems-Theoretic Process Analysis of space launch vehicles, Journal of Space Safety Engineering, Volume 5, Issues 3–4, ISSN: 2468-8967, September–December 2018, Pages 153-183

[71] SAE J1739:2009, Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA) and Effects Analysis for Machinery (Machinery FMEA), szabvány, 2009.

[72] Schaal v. H. W.: Etherent und IP Kraftfahrzeug, Elektronik automotive (elektroniknet.de), 4. 2012 https://vector.com/portal/medien/cmc/press/PON/Ethernet_IP_ElektronikAutomotive_201204_PressArticle_DE.pdf (Letöltve:2018. 04.07)

[73] Smith D., Simpson K.: Safety Critical Systems Handbook 3th Edition, A Straight forward Guide to Functional Safety, IEC 61508 (2010 EDITION) and Related Standards, Including Process IEC 61511 and Machinery IEC 62061 and ISO 13849, ISBN: 978-0-08-096781-3, 2011

[74] Snooke N., Price C.: Automated FMEA based diagnostic symptom generation, 2012

[75] Spreafico C., Russo D., Rizzi C.: A state-of-the-art review of FMEA/FMECA including patents, Computer Science Review, Volume 25, August 2017, pages 19-28.

[76] Spreafico C., Russo D., Rizzi C.: FMEA problémaosztályok (ábra forrása): https://ars.els-cdn.com/content/image/1-s2.0-S1574013716301435-gr3_lrg.jpg

[77] Spreafico C., Russo D., Rizzi C.: FMEA témájú cikkek (ábra forrása):: https://ars.els-cdn.com/content/image/1-s2.0-S1574013716301435-gr7_lrg.jpg

[78] Stehpenson J.: System safety 2000, publisher: Van Nostrand-Reinhold, New York, NY 10003, 1991.

[79] Stephans R. A.: System safety for the 21st century, Wiley-Interscience, ISBN: 0-471-44454-5, 2004

[80] Struss P., Fraracci A.: Automated Model-based FMEA of a Braking System, . 8th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes (SAFEPROCESS) August 29-31, 2012. Mexico City, Mexico

[81] The Reynolds and Reynolds Company: 2015 Auto Accessories Sales Annual Trend Report, 2016 http://universalcomputersys.com/collateral/flyers/AoA_Trend_Report.pdf (Letöltve: 2018.04.07)

[82] S. Thrun: Google's driveless car, TED2011 https://www.ted.com/talks/sebastian_thrun_google_s_driverless_car?language=en (Letöltve:2018. 04.07)

[83] TüV Nord: HARA definíciója, https://www.tuev-nord.de/en/functional-safety/our-services/hazard-and-risk-analysis/hara/ (Letöltve:2018. 04.07)

[84] US Patent No. 7197427 B2, 2007 https://patentimages.storage.googleapis.com/94/15/41/ce5077c99998a3/US7197427.pdf (Letöltve:2018. 04.07)

[85] Varga Z., Szauter F.: Járműmechatronika, (2011) Széchenyi István Egyetem http://www.tankonyvtar.hu/hu/tartalom/tamop425/0007_09-jarmumechatronika/3_lecke_az_abs.html (Letöltve: 2017.05.17)

[86] VDA 4 Quality Management in the Automotive Industry, Quality Assurance before series production, 1st edition, 1996, pp 12-16

[87] VDA bemutatása, https://www.vda.de/en/association/organization.html (Letöltve: 2017.05.17)

[88] VDA QMC (Qualiäts Management Center): FMEA Alignment VDA and AIAG 2018, http://vda-qmc.de/fileadmin/redakteur/Publikationen/FMEA_Harmonisierung/FMEA_Alignment_AIAG_and_VDA_-_ENG.pdf (Letöltve:2018. 04.07)

[89] Ved P., Deepak K., Rakesh R.: Statistical Process Control, IJRET, ISSN:2319-1163, vol2, issue 08, 2013

[90] J. W. Vincoli: Basic guide to system safety, second edition ISBN: 9780471722410, 2006.

[91] Wentao W. and Z. Hong, "FMEA for UML-Based Software," 2009 WRI World Congress on Software Engineering, Xiamen, 2009, pp. 456-460. doi: 10.1109/WCSE.2009.342

[92] Wie zuverlässig sind unsere Autos? - ADAC Pannenstatistik 2017,

[93] Wynn J., Whitmore J., Upton G., Spriggs L., McKinnon D., McInnes R., Graubart R., Clausen L.: Threat Assessment&Remediation Analysis (TARA), Methodology description v1.0, Mitre Corporation, 2011 pp10-11 https://www.mitre.org/sites/default/files/pdf/11_4982.pdf (Letöltve:2018. 04.07)

8.2 A Jelölt értekezésével kapcsolatos publikációi

[94] L. Palkovics, **G. Ványi**, A. Kovács,: Szoftver a jövő járművében, Jövő járműve, V. évfolyam, ISSN 1788-2699, 03/04sz, 2012

[95] **G. Ványi**: Improving the effectiveness of FMEA analysis in automotive – a case study, Acta University Sapientiae, Informatica 8, 1, DOI:10.1515/ausi-2016-0005, 2016, pp82-95 (Scopus)
Idézetek száma: 2db

[96] L. Pokorádi, **G. Ványi**: Gépjármű fékrendszer szoftverfejlesztésének Hibafa elemzése, In: Péter T (szerk.) Innováció és fenntartható felszíni közlekedés, IFFK 2016 . Konferencia helye, ideje: Budapest , Magyarország , 2016.08.29 -2016.08.31. Budapest: Magyar Mérnökakadémia (MMA), 2016. pp. 206-209.

[97] L. Pokorádi, **G. Ványi**: Analyzing new generation brake system's software development process by LFTSM, Computational Intelligence and Informatics (CINTI), 2016 IEEE 17th International Symposium on Computational Intelligence and Informatics (CINTI), 2016 (Scopus)

[98] **G. Ványi**: OPTIMIZING TESTS AND RELIABILITY IN AUTOMOTIVE, In: Keresztes Gábor (szerk.), Tavaszi szél 2016: Nemzetközi multidiszciplináris konferencia: Absztraktkötet . 485 p.
Konferencia helye, ideje: Budapest , Magyarország , 2016.04.15 -2016.04.17.
Budapest.
Doktoranduszok Országos Szövetsége, 2016. p. 330.
(ISBN:978 615 5586 04 0)

[99] **G. Ványi**, L. Pokorádi: Sensitivity analysis of FMEA as possible ranking method in risk prioritization, Polytechnical University of Bucharest. Scientific Bulletin. Series D: Mechanical Engineering, 80:(3)pp 165-176. (2018) (Scopus)
Független idézetek száma: 2db

[100] L. Pokorádi, **G. Ványi**: Sensitivity Investigation of Failure Mode and Effect Analysis, Vehicle and Automotive Engineering 2, Springer International Publishing, ISBN: 978-3-319-75676-9, 2018 (Scopus)

8.3 A Jelölt értekezéséhez nem kapcsolódó publikációi

[101] A. Skrabák, **G. Ványi**: AEBS interface EBS fékrendszerekben és funkcionális biztonsági vonatkozásai, MM MŰSZAKI MAGAZIN 2015/4: pp. 58-63. (2015)

[102] **G. Ványi**: Elektronikus fékrendszerek fejlesztése haszongépjárművekre, pp. 12-13. Megjelenés: Chamion Truck&Bus 2014/1 (2014)
Független idézetek száma: 1db

[103] **G. Ványi**, N. Gut, J. Kretschmer, K. Moeller: Concept study of a nonlinear mechanical lung simulator, In: Balazs Benyo , David Feng , J Geoffrey Chase , Steen Andreassen , Ewart Carson , Levente Kovacs (szerk.), Proceedings of 8th IFAC Symposium on Biological and Medical Systems . 539 p., Konferencia helye, ideje: Budapest , Magyarország , 2012.08.29 -2012.08.31. New York: Curran, 2012. pp. 149-153. (ISBN:9781622763719; 978-3-902823-10-6) (Scopus)
Idézetek száma: 1db

[104] **G. Ványi**, N. Gut, J. Kretschmer, Z. Zhao, H. Zhu , K. Möller, Design of a mechanical lung simulator - A concept study: The 6th International Conference on Bioinformatics and Biomedical Engineering (iCBBE 2012), May 17 - 20, Shanghai, China, pp. 767-770. 2012
Idézetek száma: 6db

RÖVIDÍTÉSJEGYZÉK

ADAC – Allgemeiner Deutscher Automobil Club – Német Autóklub

AIAG Automotive Industry Action Group

AP - Action Priority

ASIL – Automotvie Safety Integrity Level

CAN - Controller Area Network

CC – Critical Characteristic

CL - cause level

D - Detection

DL - design level

DML - Data Management Layer

EL - Effect level

EoL – End of Line (test)

ESP - Electronic Stability Program

ETA – Event Tree Analysis

EU – Európai Unio

FMEA - Failure Method and Effect Analysis

FTA - Failure Tree Analysis

HARA – Hazard and Risk Analysis

HAZOP – Hazard and Operability Study - veszély-és kockázatelemzés

HW - Hardware

IEC – International Engineering Consortium

IREB - Interantional Requirement Engineering Board

ISO – International Organisation for Standardization

LFTSM – Linear Fault Tree Sensitivity Modeling

LIN – Local Interconnect Network

Mech - Mechanika

NASA – National Aeronuatics and Space Administration

O - Occurence

PROMETHEE - Reference Ranking Organization Method for Enrichment Evaluations

RPN – Risk Priority Number

S - Severity

SAE – Society of Automotive Engineers

SC – Special Characteristic

SL- System level

SPC – Statistical Process Control

SW - Software

TED – Technology, Entartainment, Design (konferencia)

VDA - Verband Der Automobilindustrie

TÁBLÁZATJEGYZÉK

ÁBRAJEGYZÉK

KÖSZÖNETNYILVÁNÍTÁS

Ez úton szeretném megköszönni az Óbudai Egyetem - Gépész és Biztonságtechnikai Kar munkatársainak az értekezésem elkészítéséhez nyújtott segítségüket. Szeretném külön megköszönni témavezetőmnek a disszertáció megírásához nyújtott önzetlen szakmai- és oktatói segítségét.

Ugyancsak szeretném megköszönni családomnak a személyes támogatásukat és bátorításukat az értekezés megírásában.

SDG!