Gépjármű fékrendszer szoftverfejlesztésének Hibafa elemzése

Pokorádi László*, Ványi Gábor**

** Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar,*
1081 Budapest, Népszínház utca 8. (e-mail: pokoradi.laszlo@bgk.uni-obuda.hu)
*** Eötvös Lórnd Tudományegyetem, Informatikai Kar*
1117. Budapest, Pázmány Péter sétány 1/C (e-mail: vanyig@ceasar.elte.hu).

Kivonat: Egy tradicionálisan gépészeti megoldásokat alkalmazó iparág, a haszongépjárművek fejlesztése egyre növekvő szinten alkalmazza az elektronikus hardverek és az azokat működtető beágyazott szoftverek alkalmazását. A fő cél, hogy csökkentsék a járművek tömegét, de ugyanakkor több kényelmi- és biztonsági funkciót is valósítsanak meg. A funkciók számának növekedésével azonban a komplexitás is nő. Elvárás az, hogy ennek ellenére az elvárásoknak megfelelően, jól működjenek a rendszerek, ezért különös hangsúlyt kapnak a megbízhatósági vizsgálatok, az előzetes hibaforrás elemzések. Ezáltal a komplex rendszerek működését egyre mélyebben szükséges megismerni, mivel gyakran a teljesítményük határán üzemeltetik azokat. Felmerül tehát a kérdés, hogy miként lehetséges egy, a rendszer működését érzékenyen befolyásoló elemet kiszűrni? Ezen tanulmány egy objektív módszert kíván bemutatni a hibafa analízis segítségével, amely egy FMEA elemzés adataira támaszkodik. A bemutatandó példa az autóipari ISO 26262 funkcionális biztonsági szabványból kiinduló a szoftverfejlesztés elemi hibáit veszi alapul és vizsgálja azok kritikusságát az FMEA elemzésből kapott adatokra támaszkodva.

1. BEVEZETÉS

Napjaink mérnöki tudományában egyre nagyobb szerepet kap a bonyolult, integrált rendszerek, különféle hálózatok struktúrájával és a bennük lejátszódó folyamatok megbízhatóságának vizsgálata. Ez vonatkozik az új technikai rendszerek fejlesztésére is. Ezért fontos kérdésként merült fel annak elemzése, hogy mely elemi hiba-okokra a legérzékenyebb egy teljes rendszer vagy folyamat megbízhatósága.

A biztonságkritikus, nagy megbízhatósági igényű fékrendszerek kockázatkezelésére az IEC 61508 (IEC, 2010) szabvány adott korábban előírásokat az elemzési folyamatokra és kockázatkezelésre. Nemrég közzétették az erre épülő ISO 26262 (ISO, 2011) szabványt, amely kimondottan az autóipari fejlesztések elektronikus hardver-, illetve szoftver komponenseire fókuszál. Természetesen a kockázatelemzés és kezelés – a korábbi szabványra épülve – itt is definiálásra került. Egy fékrendszer az új szabvány elemzése alapján is magas szintű kockázatot képvisel (besorolása alapján ASIL D, amely a legmagasabb). Természetesen a legmagasabb kockázati szint több erőforrást igényel a fejlesztés folyamán, mint egy hasonló bonyolultságú, de nem biztonságkritikus beágyazott rendszer. A megnövekedett költségek ellenére is fontos a lehetséges fejlesztési utakat időben azonosítani, mert a funkciókon túl egy elérhető minőségi szintet is jelentenek.

A hibafa-elemzés során egy valós vagy feltételezett rendszerhibából, az úgynevezett főeseményből (Top Event) indulunk ki, és fokozatosan derítjük fel azokat az alkotóelem és részrendszer meghibásodási lehetőségeket, melyek az adott, nem kívánt esemény bekövetkezéséhez vezetnek vagy vezethetnek. Az elemző munkát fastruktúrájú gráf megjelenítés segíti, amit különböző, például megbízhatósági számításokkal is ki lehet egészíteni. Módszertanát az IEC 1025 (IEC, 1990) és MSZ EN 1050 (MSZ, 1999) szabványokból tudjuk

A hibafa-elemzés során egy feltételezett rendszerhibából, az úgynevezett főeseményből (Top Event) indulunk ki, és fokozatosan derítjük fel azokat az alkotóelem és/vagy részrendszer meghibásodási lehetőségeket, melyek az adott, nem kívánt esemény bekövetkezéséhez vezetnek vagy vezethetnek. Az elemző munkát fastruktúrájú gráf megjelenítés segíti, amit különböző, például megbízhatósági számításokkal is ki lehet egészíteni. Egy (nem elemi) esemény bekövetkezési valószínűsége meghatározható az azt kiváltó események – melyek lehetnek elemi vagy alacsonyabb szintű közbülső események – bekövetkezési valószínűségeinek, illetve a köztük lévő logikai kapcsolat ismeretében

Jelen kutatómunka célja egy haszon-gépjármű fékrendszerének szoftverfejlesztési folyamat hibafa elemzésének elvégzése, illetve a kidolgozott szoftver-csomag lehetséges meghibásodási lehetőségein keresztül a megbízhatóság elemzése. Ezáltal a fejlesztési folyamat azon elemei kerülhetnek kiszűrésre, amelyek különösen kritikusak egy rendszer egésze számára, azaz a kritikus (legnagyobb hatású) tényezők. A módszer alapja lehet egy katalógus összeállításához is, amely hiba-hatáselemzésekben alkalmazva következtetésre ad lehetőséget a vizsgált tényezők előfordulására egy összetett rendszerben – kiszűrve egy rendszer érzékeny pontjaiként. Az itt bemutatott példában egy hiba redundánsan (kétszer) kerül felírásra, tesztelve a kiszűrés hatékonyságát.

A tanulmány az alábbi fejezetekből áll: A 2. fejezet a vizsgált szoftverfejlesztést, és annak hibafa elemzését mutatja be. A 3. 4. fejezetben a hibafa érzékenységének meghatározása kerül

bemutatásra. a 4. fejezetben a vizsgálati eredmények kiértékelése olvasható. Végezetül a tanulmány összefoglalással zárul.

2. A VIZSGÁLT SZOFTVERFEJLESZTÉS HIBAFA ELEMZÉSE

Az elvégzett hibafa elemzés tárgya egy beágyazott rendszerben előforduló, szoftverfejlesztési folyamat hátteréből eredő szisztematikus hibák elemzése az ISO26262 szabvány alapján, miszerint egy szoftverrendszer hibája elsősorban ilyen hibákból adódik. A vizsgált nemkívánatos esemény maga a konstrukció egészének helytelen működése (v.ö. design fails), míg az elemi eseményeit egy hiba-hatás elemzés (FMEA) elkészítésekor összegyűjtött, a szoftverkomponensek meghibásodását kiváltó hibák okai alkotják. Az elemi események előfordulási valószínűségét egy rendszer funkcióinak meghibásodását előidéző okoknak az előfordulási értékeit egy hiba-hatáselemzés módszertanon alapuló táblázatból kerülnek kiolvasásra. Ezt 1-10 skálán értékelik, melyhez a SAE J-1739 (SAE, 1995), Amerikai Egyesült Államokban közzétett szabvány katalógusának 1000 járműre kivetített értéke alapján (mint populációként) kerül meghatározásra. Az egyes elemi hibák bekövetkezési valószínűségének meghatározása az előfordulási érték átkonvertálásával történt.
Az elemzésben szereplő elemi hibák (1 és 8 közötti számokkal jelölve) az 1. Táblázat mutatja a bekövetkezési amely a már említett SAE J-1739 szabvány katalógus segítségével kerültek meghatározásra hiba-hatáselemzésből.

1. Táblázat Elemi események és előfordulási értékei

i	Hiba típusa	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

A nem elemi eseményeket szintjük és sorszámuk alapján rendre „*mn*”-el indexel jelöltük, ahol *m* a sor, *n* az oszlopszám azonosítója, a főeseményt pedig *TE* jelöli. A hibafa az 1. ábrán látható.
A nem elemi események kiszámítása a hibafa elemzéshez használt *VAGY*, illetve *ÉS* kapuk felhasználásával határozhatóak meg, az alábbiak szerint:

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

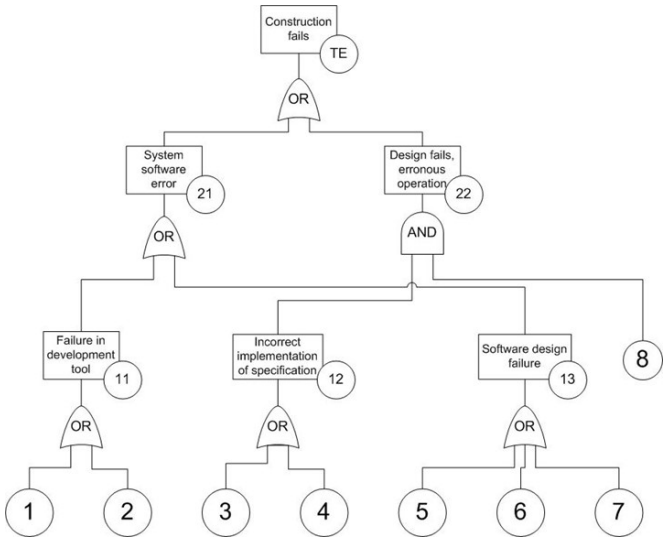
$$P_{21} = 1-\left((1-P_{11})(1-P_{13})\right) \tag{2}$$

$$P_{22} = P_{12}P_8 \tag{3}$$

$$P_{11} = 1-\left((1-P_1)(1-P_2)\right) \tag{4}$$

$$P_{12} = 1-\left((1-P_3)(1-P_4)\right) \tag{5}$$

$$P_{13} = 1-\left((1-P_5)(1-P_6)(1-P_7)\right) \tag{6}$$



1. ábra A vizsgálati hibafa

A (6) – (1) egyenletek segítségével kiszámított nem elemi események valószínűségi értékeit a 2. Táblázat tartalmazza.

2. Táblázat Számított nem elemi események értékei

i	Valószínűség
TE	0,0225
21	0,0224
22	0,0000075
11	0,0025
12	0,015
13	0,02

3. A HIBAFA ÉRZÉKENYSÉGVIZSGÁLATA

Az érzékenységi elemzés segítségével meghatározható a fő esemény bekövetkezésének szemszögéből legkritikusabbnak tekinthető elemi esemény. Pokorádi [3] tanulmányában ismertet egy mátrixalgebrai módszert, amely a logikai kapukhoz kapcsolódó valószínűségek alapján (lásd (1) – (6) egyenletek) határozza meg azok érzékenységi függvényeit, az alábbi általános lineáris egyenlettel:

$$\delta y = K_1\delta x_1 + K_2\delta x_2 + ... + K_k\delta x_k \tag{7}$$

ahol δ a változók relatív eltéréseit jelzik.
Az érzékenységi együtthatók a hibafa elemzés során, általános formában

„ÉS” kapu esetén:

$$K_i = 1 \quad \forall i \in \{1,2,...,k\} \tag{8}$$

„VAGY” kapu esetén:

$$K_j = \frac{P_j}{P} \prod_{\substack{i=1 \\ i \neq j}}^{k} (1 - P_i) \quad \forall j \in \{1,2,...,k\} \tag{9}$$

Az (1) – (6) egyenletekből az adott csomópont logikai kapujának, illetve az elemi események bekövetkezési valószínűségei ismeretében:

$$\begin{aligned} \delta P_{TE} &= K_{21}\delta P_{21} + K_{21}\delta P_{21} \\ K_{21} &= \frac{P_{21}}{P_{TE}}(1 - P_{22}) \\ K_{22} &= \frac{P_{22}}{P_{TE}}(1 - P_{21}) \end{aligned} \tag{10}$$

$$\begin{aligned} \delta P_{21} &= K_{11}\delta P_{11} + K_{13}\delta P_{13} \\ K_{11} &= \frac{P_{11}}{P_{21}}(1 - P_{13}) \\ K_{13} &= \frac{P_{13}}{P_{21}}(1 - P_{11}) \end{aligned} \tag{11}$$

$$\begin{aligned} \delta P_{22} &= K_{12}\delta P_{12} + K_8\delta P_8 \\ K_{12} &= 1 \quad K_8 = 1 \end{aligned} \tag{12}$$

$$\begin{aligned} \delta P_{11} &= K_1\delta P_1 + K_2\delta P_2 \\ K_1 &= \frac{P_1}{P_{11}}(1 - P_2) \\ K_2 &= \frac{P_2}{P_{11}}(1 - P_1) \end{aligned} \tag{13}$$

$$\begin{aligned} \delta P_{12} &= K_3\delta P_3 + K_4\delta P_4 \\ K_3 &= \frac{P_3}{P_{22}}(1 - P_4) \\ K_4 &= \frac{P_4}{P_{22}}(1 - P_3) \end{aligned} \tag{14}$$

$$\begin{aligned} \delta P_{13} &= K_5\delta P_5 + K_6\delta P_6 + K_7\delta P_7 \\ K_5 &= \frac{P_5}{P_{13}}(1 - P_6)(1 - P_7) \\ K_6 &= \frac{P_6}{P_{13}}(1 - P_5)(1 - P_7) \\ K_7 &= \frac{P_7}{P_{13}}(1 - P_5)(1 - P_6) \end{aligned} \tag{15}$$

Az elemzendő hibafa eseményeinek bekövetkezési valószínűségeit két vektorba kell rendezni, azok típusa szerint csoportosítva, külön a nem elemi és elemi eseményeket:

$$\mathbf{y}^T = [P_{TE} \quad P_{21} \quad P_{22} \quad P_{11} \quad P_{12} \quad P_{13}] \tag{16}$$

$$\mathbf{x}^T = [P_1 \quad P_2 \quad P_3 \quad P_4 \quad P_5 \quad P_6 \quad P_7 \quad P_8] \tag{17}$$

A vektorok segítségével felírhatóak a bekövetkezési valószínűségek relatív változásainak együttható mátrixai:

$$\mathbf{A} = \begin{bmatrix} 1 & -K_{21} & -K_{22} & 0 & 0 & 0 \\ 0 & 1 & 0 & -K_{11} & 0 & -K_{13} \\ 0 & 0 & 1 & 0 & -K_{12} & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{18}$$

$$\mathbf{B} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & K_8 \\ K_1 & K_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & K_3 & K_4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & K_5 & K_6 & K_7 & 0 \end{bmatrix} \tag{19}$$

Ekkor az események bekövetkezési valószínűgégei relatív változásai közti kapcsolat az

$$\mathbf{A}\,\delta\mathbf{y} = \mathbf{B}\,\delta\mathbf{x} \tag{20}$$

mátrixalakban adható meg. Ezt átrendezve kapjuk meg a

$$\mathbf{D} = \mathbf{A}^{-1}\mathbf{B} \tag{21}$$

úgynevezett relatív érzékenység mátrixot.
A mátrix *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.

4. A VIZSGÁLATI EREDMÉNYEK KIÉRTÉKELÉSE

A fenti vizsgálattal kapott relatív érzékenységi mátrix:

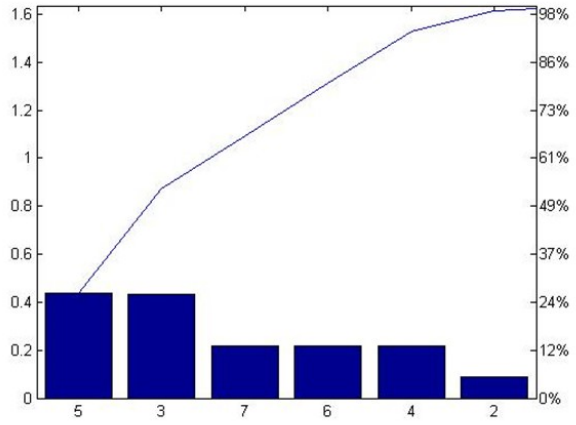
$$\mathbf{D} = \begin{bmatrix} 0{,}0218 & 0{,}0872 & 0{,}4331 & 0{,}2155 & 0{,}4398 & 0{,}2188 & 0{,}2188 & 0{,}0003 \\ 0{,}0218 & 0{,}0218 & 0 & 0 & 0{,}4398 & 0{,}2189 & 0{,}2189 & 0 \\ 0 & 0 & 0{,}0013 & 0{,}6621 & 0 & 0 & 0 & 1 \\ 0{,}1997 & 0{,}7999 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0{,}0013 & 0{,}6621 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0{,}4950 & 0{,}2463 & 0{,}2463 & 0 \end{bmatrix} \tag{22}$$

A mátrix első sora különösen fontos, mivel a főesemény bekövetkezési valószínűségének az elemi események bekövetkezési valószínűségeivel szembeni érzékenységi együtthatókat adja meg. A **D** mátrix ezen sorát, mint relatív érzékenységi (sor)vektora kezelendő, és $\mathbf{d}^T$ -vel jelve az alábbi sor írható fel:

$$\mathbf{d}^T = [0{,}0218 \quad 0{,}0872 \quad 0{,}4331 \quad 0{,}2155 \quad 0{,}4398 \quad 0{,}2188 \quad 0{,}2188 \quad 0{,}0003] \tag{23}$$

A főesemény relatív érzékenységvektora egy Pareto elemzéssel értékelhető ki, kiemelve a legkritikusabb elemet. A Pareto diagram érzékelhető eloszlást mutat várhatóan a legkritikusabb hiba okokról. A kapott eredmények alapján két hiba emelkedik ki:
– rendszer specifikáció követelményeit hibásan kerül implementálásra;

illetve
– hibásan implementált követelmények (interfész szempontjából).



2. ábra Pareto elemzés az elemi események bekövetkezése alapján

A két hiba a fejlesztés alapját képező követelmények hibás értelmezéséből ered, amely alátámasztja egyrészt azt az elméletet is, miszerint a szoftver önmagában nem képes meghibásodni. Ugyancsak ezt erősítik a következő, alacsonyabb szinten látható hibák is, amelyek már a feldolgozás/strukturálásra vezethetőek vissza. A fékrendszerek tervezésében ezért is került bevezetésre a követelményekből készített biztonsági tervek (Safety Concept) kidolgozása az ISO 26262 (ISO, 2011) szabvány alapján. Megjegyzendő, hogy a módszer implicit módon, pontosan a két redundánsan felírt hibát találta meg és emelte ki hasonló súllyal.

4. A VIZSGÁLATI EREDMÉNYEK KIÉRTÉKELÉSE

Az elvégzett elemzés igazolta, hogy a lineáris hibafa érzékenységi modell jól alkalmazható a különböző műszaki rendszerek elemzésére, mint például a biztonságkritikus rendszerek, illetve az ahhoz kapcsolódó fejlesztési folyamatok érzékenységi pontjainak azonosítására. A könnyen algoritmizálható elemzési eljárás eredményei rámutattak az újgenerációs fékrendszerek szoftver fejlesztési folyamatának egy-egy érzékeny pontjára. Ezáltal részben bizonyítást nyert az ISO szabványban definiált ajánlás létjogosultsága, amely egyes követelmények megjelölését/kiemelését ajánlja biztonságkritikusként. Ezáltal azok teljesülése kiemelt figyelemmel külön tesztelhető, illetve validálható egy-egy fejlesztési iteráció végén.
A bemutatott hibákból egy katalógus bevezetése is gyorsíthatja a kiértékelést. Használata egy esetleges visszacsatolás beiktatása a meghibásodásokkal-tovább növelheti az érzékenységvizsgálat hatékonyságát. Ezáltal az ehhez hasonló elemzés eredményeként a levont következtetések alapján a megbízhatóságot, és így a biztonságot növelő intézkedések hozhatók.

5. ÖSSZEFOGLALÁS

A tanulmányban bemutatott módszer alkalmazása kiterjeszthető több, hasonló szintű tesztek vagy vizsgálati események objektív kiválasztására valamely súlyozási feltételek alapján.
A Szerzők egy autóipari alkalmazást mutattak be, összekapcsolva a kötelezően alkamazandó elemzési eszközöket. Itt a kiválasztáshoz az FMEA elemzésből jövő, kiértékelt adatokra támaszkodtunk, amely ugyancsak hasznos lehet egy rendszer tesztjeinek rangsorolásának felállításához is. Ez esetben a Pareto elemzés által kiemelkedő hibák akár a regressziós teszt részei lehetnek, míg a kevésbé kiemelkedő hibákat egy fejlesztési ciklusban elegendő lehet kevesebbszer futatni – időt és költséget megtakarítva. A könnyű algoritmizálhatóság miatt ez a módszer hatásos eszköz a megbízhatósági számításokban, hiszen kezelhető mérnöki számítását végző programok által is (például Matlab) és gyorsan eredményekhez juthatunk jelentősebb számítási kapacitásigény nélkül.

REFERENCES

IEC 1025 (1990) Fault tree analysis (FTA), International Electrotechnical Commission, Genf 39.
IEC 61508 (2010) *Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-related Systems* International Electrotechnical Commission Genf
ISO 26262 (2011) *Road vehicles – Functional safety.* International Organization for Standardization"
MSZ EN 1050 (1999,) *Gépek biztonsága – A kockázatértékelés elvei*., Magyar Szabványügyi Testület, Budapest.
Pokorádi, L. (2011) Sensitivity Investigation of Fault Tree Analysis with Matrix-Algebraic Method, *THEORY AND APPLICATIONS OF MATHEMATICS & COMPUTER SCIEN-CE* **vol. 1:(1)** 34-44.
SAE J-1739 (2013) *Potential Failure Mode and Effects Analysis in Design (Design FMEA), Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA)*