Műszaki okú kockázatok kezelése a közlekedésben

Szabó Géza
BME Közlekedésautomatikai Tanszék
1111 Budapest, Bertalan L. u. 2.
szabo.geza@mail.bme.hu

Absztrakt

A cikk bemutatja az összes kockázatos emberi tevékenység végrehajtásánál, így a közlekedésben is egyre fontosabb szerepet kapó kockázati alapú követelmények specifikálásának folyamatát és problémáit. A cikk a kockázatok műszaki okainak menedzselésével foglalkozik és nem tárgyalja a folyamat végrehajtása alatti emberi okú kockázatokat, noha a technika fejlődésével ma már olyan szinten állunk, ahol a műszaki rendszerek meghibásodásából eredő veszteségek jóval csekélyebbek az emberi okú veszteségeknél. A közlekedésben a műszaki részt a járműrendszerek és a pályamenti elemek képviselik.

A cikk foglalkozik a kockázati paraméterek fejlesztésre, illetve tágabb értelemben a pályamenti elemek vagy a járművek teljes életciklusára gyakorolt hatásával, és hangsúlyozza a teljes életciklusban részt vevők kockázati alapú gondolkodásának szükségességét. A kérdés azért is nagyon fontos, mert elsősorban a közúti járműveknél a járművek életciklusában sok nem szakember vesz részt. Ezen résztvevőknek is érteniük kell azonban azt, milyen alapokon, milyen feltételekkel kerültek meghatározásra a biztonsági paraméterek, miért ilyen módon és milyen következményekkel járnak ezek az üzemeltetésre.
Mivel a kockázati alapú követelmények bevezetését a teljes életciklusban elkövethető emberi okú hibák elleni védekezés motiválta, a kritériumok bevezetésének nagy hatása van az életciklusra, elsősorban a termékek fejlesztésére. A kritériumoknak való megfelelés könnyebbé tétele, és ezen keresztül az erre fordítandó humán és anyagi erőforrások csökkentése érdekében fejlesztés támogató informatikai rendszert célszerű alkalmazni - cikkünk felvázolja egy ilyen rendszer fő funkcióit.

The paper introduces the process of the risk estimation based safety requirements specification applied for all the human activity which can cause danger. One of these dangerous human activities is transportation and traffic control. The paper deals with the technical aspects only and not covers the human errors during the dangerous activity. We must know that – because of the technical development – the risk originates from the technical systems is much lower than the risk of using them (human activity). In transportation, the technical parts can be the track-side elements and the vehicle systems.

The paper deals with the effects of the specified safety requirements to the development and the activities in the whole life-cycle and emphasizes the importance of the risk based mind of the participants in the life-cycle both professionals and inexpert like costumers of vehicles. These people also must know on which base, with which conditions the safety parameters are determined and what the consequences of these parameters are to the operation and maintenance.
As the introduction of the risk based criterion was initiated by the prevention of the human errors caused during the activities in different life-cycle phases, the criterion has a great influence to the whole life-cycle, mainly to the development. To make the fulfillment of the criterion more easy, and through this to decrease the human and economic resources needed, an information system supporting risk based development shall be applied - our paper summarizes the main functions of this information system.

1. Bevezetés

A nagy biztonságú rendszerek fejlesztői, ellenőrei, jóváhagyói és üzemeltetői kénytelenek voltak szembenézni az elektronikus, programozható elektronikus rendszerek terjedésével előtérbe kerülő problémával, a rendszer működésében keletkező, nem a hardver meghibásodásából, hanem hibás emberi tevékenységekből (téves specifikálás, hibás tervezés, elégtelen ellenőrzés és tesztelés vagy üzemeltetés stb.) származó funkcióvesztéssel. Ez a probléma azért is jelentős, mert a rendszerek bonyolódásával azok működési állapottere is robbanásszerűen nő, és ez az ellenőrzéshez szükséges, reprodukálható, objektív tesztelési esetek számának az elfogadhatón túli növekedését jelenti. Tehát szembe kellett nézni azzal a ténnyel, hogy a korszerű, nagy bonyolultságú rendszerek nem tesztelhetőek ki teljes körűen.

Fel kellett ismerni azt a tényt, hogy a biztonságot fokozó rendszerek sem lehetnek tökéletesek, „abszolút biztonság nem létezik". Természetesen lehet a biztonságot minden határon túl növelni, de valamekkora működési kockázat, biztonsághiányos állapot lehetősége mindig fenn fog állni. Ráadásul a biztonság növelése egyre nagyobb és nagyobb ráfordításokat igényel, így gondolni kell a megfizethető biztonságra is (Példák erre a személygépkocsik biztonsági felszerelései: egy adott vásárló az ár, illetve saját kockázattűrő képességének ismeretében dönt a személygépkocsi megvásárlásakor a megrendelendő biztonságot fokozó berendezésekről is. Számtalan példát látunk arra, hogy valaki légzsákok nélkül vásárol autót, noha azok kedvező hatása mindenki számára ismert.)

A fentiek ismerete, illetve figyelembe vétele a közlekedésben is nagyon fontos. A vasúti és légiközlekedés a kockázati alapú megközelítéseket már régóta alkalmazza, és napjainkban már a közúti közlekedésben részt vevő járművek gyártói is ilyen elvek mentén határozzák meg az alrendszerek biztonsági követelményeit. Az elektronikus fékekre vagy kormányrendszerekre vonatkozó fejlesztések tervezésénél, kivitelezésénél a kockázati alapú megközelítés nem csak fontos, de hasznos is. Ugyanakkor ki kell jelentenünk azt is, hogy a kockázati alapú gondolkodás, illetve a fejlesztés ilyen ismérvei nem csak a gyártók számára (meg)ismerendő területek. Ismernie kellene ezt minden, a járművek életciklusában részt vevő szereplőnek, így az engedélyezési eljárások résztvevőinek és az üzemeltetőknek (személygépkocsiknál a széles fogyasztói rétegnek) is.

A terület fontosságát mutatja, hogy napjainkra általános (pl. EN 61508 [1]) és ágazatspecifikus (pl. vasúti területen az EN 50126 [2], lásd még [3]) szabványok is részletesen foglalkoznak a kérdéssel.

Cikkünkben bemutatjuk a biztonsági követelmények kockázati alapú specifikálását, a specifikált értékek fejlesztésre, illetve a rendszer életciklusára gyakorolt hatását, majd vázoljuk egy, a kockázati alapú követelményekkel is rendelkező fejlesztést támogató információs rendszer koncepcióját.

2. Biztonsági követelmények kockázati alapú specifikálása

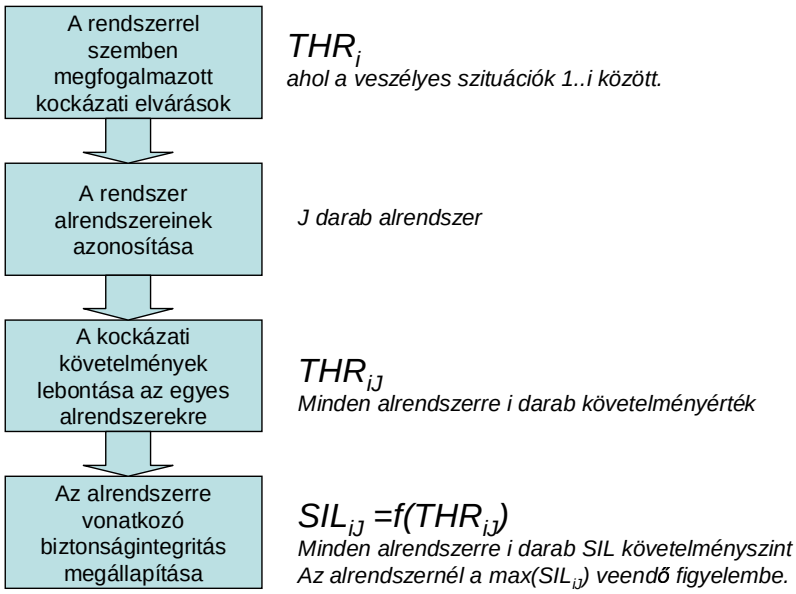
A korai rendszereknél elsősorban a rendszer, vagy annak komponensei hardver okú meghibásodásából származó funkcióvesztéssel számoltak. Természetes tehát, hogy ekkoriban a rendszer biztonságosságát a hardver jóságával (meghibásodási gyakoriságával vagy valószínűségével) azonosították. Egy adott rendszert tetszőleges fokúan hibatűrővé lehet tenni a hardver meghibásodások hatásai ellen: redundancia alkalmazásával elkerülhetőek a nem kívánt hatások (fault-tolerant technika), vagy hibafelismerés esetén a rendszert biztonsági állapotba lehet vezérelni (fail-safe technika). Természetesen a hardver jósága továbbra is fontos paraméter, a teljes rendszer veszélyes állapotot okozó meghibásodási rátáját meg lehet feleltetni az un. eltűrhető veszélyességi rátának (Tolerable Hazard Rate, THR).

Ahogy a bevezetőben már említettük, a hardver meghibásodások mellett egyre nagyobb szerepet kapnak a helyesen működő rendszerelemek mellett bekövetkező funkcióvesztések. Ezeket minden esetben valamilyen téves emberi cselekvésre lehet visszavezetni (pl. hibás feladat-meghatározás vagy karbantartási hiba). Ezek a téves tevékenységek ellen is védekezni kell – sajnos ahogy a hardver meghibásodások jól számszerűsíthetők, az itt említett hibák kvantitatív módon nehezen kezelhetőek Éppen ezért terjedt el az ilyen hibák elleni védekezésnél az osztályba sorolás (biztonságintegritási szint – Safety Integrity Level, SIL).

Természetszerűleg a THR és SIL értékeknek összhangban kell lenniük: Nem érdemes olyan rendszert gyártani, amely a hardver meghibásodások ellen nagyfokúan védett, de tele van emberi hibákkal, és ezért gyakran tévesen hajt végre funkciókat, mint ahogy az sem jó megoldás, hogy egy emberi hibák ellen nagyfokúan védett rendszert gyenge hardveren valósítunk meg. Az összerendelés módja triviális:

a számszerűen is meghatározott THR érték alapján választjuk ki a THR értéknek megfelelő SIL szintet.

A THR érték meghatározásánál az eltűrhető kockázatból (vagy kockázatokból) kell kiindulnunk: maga a kockázat a veszélyes állapotok gyakorisága és a veszélyes állapotokhoz tartozó lehetséges kár függvénye.
Alapszituációban a rendszer az általunk elviselhetőnél magasabb kockázatokat rejt magában, ezt kell csökkentenünk a berendezéseinkkel legalább az elviselhető szintre (és megfontolandó, hogy ne túlzottan az elviselhető szint alá, mert az ilyen megoldásnak a költségvonzatai lesznek jelentősek és nem tolerálhatóak). Ezt a kockázatcsökkentést a beépített védelmi berendezéseink által kell biztosítani, és a kockázatcsökkentés számszerű követelménye meg is határozza a már korábban említett biztonságintegritási követelményt is.
Az 1. ábra egy rendszer alrendszereire (alrendszernek tekinthető például fékrendszer egy járművön; de független elektronikus és pneumatikus fékrendszerek esetén önálló alrendszer az elektronikus fék) vonatkozó követelmények megállapításának folyamatát mutatja.



1. ábra: A biztonsági követelmények meghatározásának folyamata

Az 1. ábra szerinti eljárásban először a teljes rendszerrel (pl. egy gépjárművel) szemben támasztott kockázati kritériumokat kell meghatározni. Itt minden esetben a funkciókból kell kiindulni, illetve a funkciók nem, vagy téves teljesülése esetén figyelembe veendő következményekkel kell számolni. A következmények veszteségben (emberélet, anyagi vagy természeti javak stb.) történő kifejezése és egy, a társadalom által eltűrt értékhez viszonyítása segítségével megállapítható, hogy az adott funkcióhiba milyen gyakorisággal engedhető meg. ennek a megengedett értéknek az elnevezése az „Eltűrhető Veszélyességi Gyakoriság”, angolul Tolerable Hazard Rate, THR.
A funkciók sokfélesége miatt egy adott rendszerre többféle kockázati követelmény is támasztható, értelemszerűen mindegyikük egy-egy funkcióhibához kapcsolódik (az ábrában ezt *i* funkciót feltételezve THR_i jelöli).
A fenti lépés legnehezebb pontját a „társadalom által eltűrt veszteség” vagy más megfogalmazásban a „társadalom által elfogadott kockázat” értékének meghatározása jelenti. Noha a szakemberek mindegyike tisztában van azzal, hogy az élet minden területe rejt magában veszélyeket (és ki ne gondolt volna abba bele – főleg egy sok közúti halálesetet produkáló nyári hétvége után – hogy beülve az autónkba velünk is történhet baleset), mégis nagyon nehéz kijelenteni azt, hogy a rendszerbe bele van kódolva a veszteség: pl. úgy tervezzük meg járműveinket, hogy – igaz nagyon, sőt a nem szakemberek számára felfoghatatlanul ritka esetként - de előfordulhatnak műszaki hibából adódó balesetek még a leggondosabb karbantartás mellett is.

Éppen ezért nagyon fontos a szakemberek és a döntéshozók felelőssége is a kockázati alapú gondolkodás társadalom felé történő kommunikálásában, illetve társadalmi elfogadtatásában! A feladat nem egyszerű és nem is népszerű, mert ki az, aki könnyen elfogadja, hogy az ő életére mások kritériumokat szabnak? Mindenesetre a dolog gazdasági oldala is fontos: az adott kockázati, illetve biztonsági szint elérése pénzbe kerül; egy magasabb szint elérése több pénzbe; és egyre kisebb biztonságemelés csak egyre nagyobb befektetések árán finanszírozható. Tehát a megfizethetőségi oldalt is figyelembe kell venni: amíg a személyt érintő közvetlen vagy közvetett gazdasági vonatkozásokra nem derül fény, addig másoktól mindenki a maximumot követelné meg a saját biztonsága érdekében. Példaként nézzük a személygépjárművek biztonsági elemeit: van, aki ABS és ESP nélkül nem vásárol autót, és van, aki ezek nélkül is használja a sajátját – nyílván az anyagi teherbíró képességének és az egyéni kockázatviselő képességének függvényében dönt a felvállalt kockázat mértékéről (feltételezve, hogy ez egy tudatos kockázati döntés) – itt mindenesetre a közvetlen gazdasági kapcsolat nyilvánvaló. Ugyanakkor egy atomerőmű biztonsági szintjének növelését is a teljes lakosság fizeti meg az energia árán keresztül, vagy a vasúti járművek biztonságnövelését a viteldíjon keresztül, a gazdasági kapcsolat mégis sokkal kevésbé nyilvánvaló.

Az eljárás második lépése a funkcionálisan független alrendszerek feltárása. Az alrendszerek kapcsolata lehet soros: ekkor bármelyikük funkcióvesztése a teljes rendszer funkcióvesztését okozhatja; és lehet párhuzamos: ekkor az összes alrendszer egyidejű funkcióvesztése szükséges a rendszerszintű funkcióvesztéshez; valamint lehet ezek tetszőleges kombinációja. Fontos megjegyezni, hogy egy adott rendszer funkciói szempontjából az alrendszerek másként és másként viselkedhetnek, adott esetben egyes alrendszerek egyes rendszerfunkciók szempontjából nem is relevánsak.
Ezen a szinten kezelhetjük a kockázatcsökkentési igényeket is: ez esetben két párhuzamos alrendszerről beszélünk, az egyik a korábbi, túl nagy kockázatú rendszer maga, míg a másik a kockázatot továbbcsökkentő, un. védelmi rendszer.
Adott esetben a rendszer alatt teljes közlekedési rendszer is érthetünk, míg más esetekben a járműszint a megfelelő kiindulási alap.

A harmadik lépésben a korábban feltárt alrendszerek közötti kapcsolatnak megfelelően a követelmények alrendszerekre lebontása történik meg. A lebontásnál figyelembe lehet venni, hogy már létező alrendszerek adott kockázati (funkcióvesztési) rátával rendelkeznek. Teljesen eredeti fejlesztésnél viszont szabad a fejlesztő keze a követelmények allokálásánál – ilyenkor azt kell figyelembe venni, hogy a különböző technológiákon alapuló, különböző bonyolultságú alrendszerekkel milyen biztonságot lehet reálisan elérni, és a magasabb kockázati követelményt az egyszerűbb, biztonságosabb alrendszerre kell kiosztani. Fontos megjegyezni, hogy párhuzamos alrendszerek esetén a rendszerrel szemben támasztott követelményeknél enyhébbek az egyes alrendszerekre lebontott követelmények, míg soros alrendszerek esetén szigorúbbak.
Az eredmény az alrendszerek egyes funkcióira vonatkozó megengedett funkcióvesztési ráta vagy valószínűség. Ezt az eredményt már a hardverrel szemben támasztott megbízhatósági követelményként kezelhetjük: mivel az alrendszer tervezése, gyártása, üzemeltetése (általánosságban: életciklusa) során elkövetett emberi hibából származó funkcióvesztés számszerűsítése nem megoldott, így azok ellen a biztonságintegritási szinten keresztül szokás védekezni, és csak a hardver meghibásodásokból származó funkcióvesztéseket számszerűsítjük.

A negyedik lépés a biztonságintegritási követelmények meghatározása az alrendszerek szintjén. Erre az előző fejezetben említett okok, az emberi vagy más néven közös okú hiba (azért nevezik így, mert azonos körülmények között minden azonos berendezésnél jelentkezik) hatásainak megfelelően alacsony szintre csökkentése, illetve a csökkentés támogatása.
A biztonságintegritás tehát szinteket takar, különböző szintű védettségi igényt a fenti hibákkal szemben. Ezért értéke (általánosságban 1-4 között, SIL4 a legmagasabb igényű) szorosan összefügg a THR szinttel, abból származtatható (példaként az EN50126 kapcsolódó, EN50129 szabványában definiált összefüggést mutatjuk be az 1. táblázatban.

THR értéke (egy órára vonatkoztatva)	SIL
$10^{-9} \leq$ THR $< 10^{-8}$	4
$10^{-8} \leq$ THR $< 10^{-7}$	3
$10^{-7} \leq$ THR $< 10^{-6}$	2
$10^{-6} \leq$ THR $< 10^{-5}$	1

1. táblázat: THR és SIL összerendelés

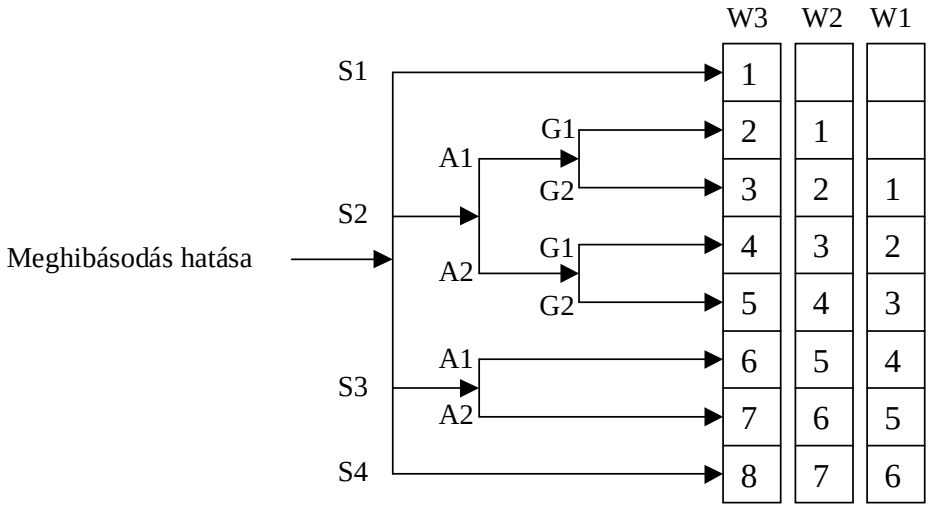
(Megjegyzés az 1. táblázathoz: A 10^{-9} értéknél szigorúbb követelménnyel rendelkező alrendszert vagy több egyedi alrendszerként, vagy járulékos kockázatcsökkentésekkel SIL4-es rendszerként kell megvalósítani.)

Ahogy egy alrendszernek több THR értéke lehet a különböző funkcióvesztésekre, úgy azokból több SIL szint is származhat az alrendszerre. Ezek közül mindig a legkritikusabbat kell figyelembe venni.

A folyamat végeredménye az alrendszerekre vonatkozó THR és SIL követelmény.

3. Alternatív módszerek

Az előző fejezetben bemutatott módszer nagy hátránya, hogy ki kell mondani, a fejlesztésnél adott veszteség (emberélet, anyagi javak) figyelembe lett véve. Egy adott szintű veszteség mértékének, de már önmagában a ténynek is az elfogadtatása nagy nehézségekbe ütközik.
Éppen ezért alkalmazzák az olyan alternatív módszereket, amelyek csak egy adott alrendszer szintjén, az alrendszer néhány paramétere alapján sorolják be az alkalmazást valamely biztonságintegritási, vagy ahhoz hasonló kategóriába (ezekben az esetekben tehát THR számítás és allokáció nem történik).
A 2. ábrán az előzőekre példaként a DIN 19250 német szabványból származó, de módosításokkal sok egyéb előírás által javasolt és sok felhasználási helyen alkalmazott kockázatértékelési gráfot mutatjuk be.



2. ábra: Biztonsági szint megállapítása DIN19250 alapon

A gráf négy (eléggé szubjektív) paramétert használ:

1. A meghibásodás által okozható kár mértéke (4 fokozat, S1-S4),
2. A veszély által érintett zónában való tartózkodás (2 fokozat, A1-A2),
3. A veszély elhárításának lehetősége (2 fokozat, G1-G2), valamint
4. A meghibásodás bekövetkezésének valószínűsége (3 fokozat, W1-W3).

Adott alkalmazáshoz a négy paraméter kategóriáinak a megfelelő megválasztásával az alrendszereket biztonsági osztályokba lehet sorolni (a 2. ábra nem SIL szerinti négy, hanem a DIN szabvány szerinti 8 kockázati osztályt alkalmaz, itt is a növekvő érték növekvő biztonsági igényeket jelent).

4. A specifikált értékek következményei

A biztonsági követelmények – a biztonsági funkciók előírásán túl – az előző fejezetben bemutatottaknak megfelelően – két kategóriába sorolhatók:

- Az alrendszerek hardver okú hibáinak korlátait specifikáló THR értékek,
- Az alrendszer közös okú hibavédettségét előíró SIL szint.

A THR értékeket többek között a hardver architektúra, az elemek kiválasztása és meghibásodási módjaik detektálásának megtervezése, valamint a szükséges karbantartási ciklusidők és az üzemeltetési körülmények specifikálása során kell figyelembe venni (Fontos, hogy az alrendszer hosszú távú biztonságát is a fejlesztés során kell megalapozni, pl. megfelelő üzemeltetési előírásokkal.

A SIL szint az alrendszer teljes életciklusát meghatározza. Speciális minőségbiztosítási rendszerrel szemben támasztott igényként fogható fel az alábbi fő pontokkal:

- Az életciklus fázisok pontos tervezése (fázisok bemeneti információi; tevékenységek az adott fázisban; az előállítandó kimeneti információk; a fázis eredményeinek verifikálása);
- Az egyes tevékenységek és eredmények (az információáramlás) szigorú rögzítése (dokumentálása);
- A folyamatokban részt vevők szakképzettségének, tapasztalatának és egymástól való függetlenségük előírása;
- Az egyes életciklus-fázisokban alkalmazandó módszerek és eljárások előírása.

Értelemszerűen a különböző biztonsági szintekhez a fenti vonatkozású követelmények is differenciáltak: a különböző SIL szintek különböző mélységű követelményeket támasztanak az előbb bemutatott négy fő pont szerint.

5. Példa kockázati alapú követelményspecifikációra

Az alábbiakban [5] alapján mutatjuk be a kockázati alapú követelményspecifikációt. Példánk a közút-vasút szintbeli kereszteződéseket biztosító fényjelző készülék fényadó eleme, az un. optika. A példa egy új korszerű technológia, a LED-es fényforrások bevezetésének támogatásához készült.

A sorompó LED optika a közút-vasút szintbeli kereszteződést biztosító berendezés része, ez a berendezés végzi az optikák vezérlését. Az optikák feladata vezérlés esetén megfelelő fényerősségű fényjel adása, vezérlés nélkül minimális (optimálisan nulla) fény kibocsátása. A biztosítóberendezés a fény kibocsátását áramfelvétel útján ellenőrzi. Amennyiben a fénykibocsátás nem biztosított, a lehetőségek szerint a vonatmozgást korlátozza vagy akadályozza.
A közút-vasút szintbeli kereszteződéseket biztosító berendezéseket több alcsoportra lehet osztani, szokásos pl. az állomási – vonali felosztás. Noha kockázat szempontjából lehetne különbséget tenni az egyes alcsoportok között, annak érdekében, hogy a fejlesztés tárgyát képező optika ne legyen specifikus valamelyik sorompótípusra, hanem bármelyikben felhasználható legyen, egységes kockázatelemzést végzünk. A kockázatelemzés során felhasználjuk azt a tényt, hogy a sorompó fényjelző készülékek két, ellenütemben villogó vörös optikát tartalmaznak.

Kockázatelemzésünk kiinduló gondolata, hogy az útátjáróban elsősorban a közúti járműveket kell védeni, a vasúti kár egy esetleges ütközés esetén a közúti kárnál nagyságrendekkel kisebb, emberélet elvesztésével is elsődlegesen a közúton kell számolni. Az elemzésnél az MSZ-EN 50126 szabvány GAMAB módszerét alkalmazzuk, amely szerint minden új rendszernek legalább olyan biztonsági szintet kell nyújtania, mint a korábbi rendszereknek.

Ismert és sajnos mindenki által elfogadott tény, hogy a közúti közlekedésben naponta négy ember hal meg. Tételezzük fel, hogy a közút-vasút kereszteződések (amelyek köztudottan a közlekedés egyik legveszélyesebb részét képezi) a napi halálozási rátának csak a 0,01 szeresét, 1%-át adják, vagyis Magyarországon útátjáró balesetben naponta 0,04 személy veszti életét. Tételezzük fel, hogy 2000 biztosított útátjáró létezik, ezek biztosítási szintje ugyan eltérő (az igazán veszélyesek minden esetben csapórúddal is biztosítottak), de számításunkban ettől eltekintünk. Ez alapján egy útátjáróban naponta $0,04/2000=2*10^{-5}$ személy halhat meg.

Az útátjáró balesetek egy részét a jól működő útátjáró mellett a közúti járművek vezetőinek felelőtlen magatartása okozza, ezért a berendezés hibájaként csak $1*10^{-5}$ személy halálát engedjük meg naponta, óránként ez kb. $4*10^{-7}$ érték. Tételezzük fel, hogy a járművezetők magatartása felelős (a felelőtlen magatartást már korábban figyelembe vettük), ezért csak minden ötödik veszélyes szituáció jár balesettel, viszont egy balesetben egynél több személy is meghalhat, a számítási egyszerűség kedvéért az egy balesetben elhunytak átlagos számát tekintsük ötnek, így $4*10^{-7}$ 1/óra adódik a veszélyes meghibásodás gyakoriságára.

Veszélyes az a szituáció, amikor a vörös jelzés szükséges lenne, és az nem jelenik meg. Ez lehetséges a vezérlő biztosítóberendezés meghibásodása miatt (pl. foglaltság-érzékelés hibája stb.). Mivel a biztosítóberendezés magas biztonsági szintű, alapvetően SIL4 szintre tervezett, ezért az ilyen hibákra csak 10^{-8} -10^{-9} hiba/óra gyakoriságot engedünk meg, ekkor az optika hibára (jó közelítéssel) továbbra is marad a $4*10^{-7}$ 1/óra érték. Itt a továbbiakban figyelembe vesszük, hogy a vörös jelzés adása két, egymástól független optikával történik, amelyek együttes meghibásodása jelent csak a szempontunkból veszélyes állapotot. Az együttes meghibásodás számításához tételezzük fel, hogy az egyedi optika meghibásodási rátája y 1/óra, így egy év alatt $365*24*y$ meghibásodással számolhatunk. Tételezzünk fel 24 órás maximális javítási időt az egyedi optika vonatkozásában (ehhez a veszélyes meghibásodásnak detektáltnak kell lennie, ez később teljesítendő), így egy év alatt $24*(365*24*y)$ hibás állapotban töltött idővel számolhatunk (feltételezve, hogy ez az idő nem lehet hosszabb egy évnél), a hibás állapot valószínűsége:

$$24*(365*24*y)/(365*24)= 24*y=P$$

A két optika együttes meghibásodásának gyakorisága:
$P*y+P*y$, feltételezve a két optika azonosságát, ennek az értéknek kell kisebbnek lennie, mint $4*10^{-7}$ 1/óra. Ebből y=**$9,12*10^{-5}$ 1/óra**.

Ez az érték a SIL1 Biztonságintegritási szintnek felelne meg. Vegyünk figyelembe azonban egy 10-es biztonsági faktort, az optika vonatkozásában írjunk elő **$9,12*10^{-6}$ 1/óra** veszélyes meghibásodási gyakoriságot. **Ez az optika vonatkozásában SIL2 értéket jelent.**
A teljes rendszer szempontjából azonban nem az a veszélyes szituáció, amikor a vörös jelzés nem jelenik meg, hanem amikor a vörös jelzés olyan módon nem jelenik meg, hogy azt a biztosítóberendezés nem detektálja.
Külön figyelmet érdemel az a szituáció, amikor a vörös jelzés nem jelenik, meg, de a fehér téves módon világít, ez azonban csak két optika egyidejű meghibásodása miatt állhat elő optika hibából, ezért ennek az egyedi optikára vetített megengedett gyakorisága az előző értéknél magasabb.

5. Néhány gondolat az egyes közlekedési ágak közötti különbségekről

A fentiekben a műszaki rendszerek biztonsági szintjének meghatározásáról értekeztünk. Fel kell azonban vetni egy globálisabb problémát is: A rendelkezésre álló (elsősorban anyagi) erőforrásokat vajon a műszaki rendszerek biztonságának növelésére kell fordítani, vagy a (cikkben nem tárgyalt) emberi hibák kiszűrésére.
A fenti kérdés nem válaszolható meg a közlekedés egészére általános módon. Figyelembe kell vennünk az ágazatok sajátosságait is:
A vasúti és légi közlekedés kevés járművel, a járműveken jól képzett és motivált, a tevékenységet szakmaként végző kezelő- vagy vezetőszemélyzettel üzemel, ráadásul a vezetőszemélyzet

ellenőrzésének lehetősége is fennáll. A belépés lehetősége magánszemélyek számára mind gazdaságilag, mind jogi értelemben nagyon lehatárolt. Az ilyen rendszerekben célszerű az erőforrásokat a technikai rendszerek fejlesztésére fordítani.

A közúti közlekedést a sok jármű, alapvetően képzetlen és motiválatlan járművezető jellemzi, a belépés lehetősége mind gazdaságilag, mind jogi értelemben nagyon könnyű (pl. használt autó vásárlása és a jogosítvány megszerzése). Az ilyen rendszerekben célszerűbbnek látszik a rendelkezésre álló erőforrások humán oldali biztonságra való fordítása.

6. A fejlesztést támogató informatikai rendszerek

A kockázati kritériumokon alapuló fejlesztések egyik kulcspontja a SIL követelmények megfelelő értelmezése, az alternatív módszerkombinációk közül a fejlesztésnek, a résztvevők tudásának, valamint a cég igényeinek legjobban megfelelő módszerkombináció megválasztása, illetve a fejlesztési folyamat megfelelőségének nyomon követése [4].
Ez a nyomon követés „manuális" módon is megvalósítható: egy erre a célra kijelölt személy (biztonsági vezető, assessor stb.) ellenőrzi a vonatkozó követelményeket, az aktuális állapotot és az előrehaladásokat. Ugyanakkor az ellenőrzéshez szükséges funkciók jól tárolhatóak informatikai rendszerekben, amelyek egyes kiértékeléseket is meg tudnak valósítani, és jelentéseket is automatikusan tudnak generálni. Ráadásul az így tárolt és feldolgozott információ a folyamatokban részt vevők számára is könnyen hozzáférhető, ezért jelentős munkaidő- és ezen keresztül gazdasági megtakarítás érhető el alkalmazásukkal.

A fejlesztést biztonságintegritási szempontból támogató informatikai rendszerektől az alábbi funkciók várhatóak el:

- Statikus funkciók (az életciklus egy adott pontján elvégzendő feladatok támogatása vagy statikus információszolgáltatás):
    1. Tegyék lehetővé az életciklus fázisok tervezését, és a fázisokra adjanak javaslatot;
    2. Tegyék lehetővé a kockázat és a biztonságintegritás meghatározását;
    3. Tegyék lehetővé a fázisokon belül a bemeneti információk, a tevékenységek és a kimeneti információk tervezését; ehhez adjanak javaslatot; az információkhoz rendeljenek megjelenési formát;
    4. Tegyék lehetővé a fázisokban alkalmazandó módszerkombinációk összeállítását; tartalmazzanak utalásokat a szabványokra az engedélyezett vagy tiltott módszerek vonatkozásában, a megkövetelt SIL szint figyelembe vételével, valamint adjanak módszertani útmutatót a módszerek alkalmazásához;
- Dinamikus funkciók (Folyamatos információgyűjtés a projektről, az adott állapotnak megfelelő jelentések létrehozása):
    1. Tegyék lehetővé a munka előrehaladtának, valamint az elkészült információk monitorozását; tiltsák meg egy adott fázis megkezdését, ha az indulás feltételei nem adottak (pl. előző fázis még nem zárult le);
    2. Nyújtsanak automatikus verziókövetést az egyes fázisokban létrejött információ módosulásáról;
    3. Kezeljenek jogosultságokat a részt vevők azonosíthatósága érdekében.
    4. Generáljanak jelentéseket a fejlesztés állásáról és egyéb követelményeknek való megfeleléséről.

Már a statikus funkciók megvalósítása jelentős segítséget nyújthat az adott alrendszer életciklusa során, de ez esetben még nem beszélhetünk többről, mint interaktív szabvány- és módszertani adatbázisról, amely a lekérdezéseknél elsődleges szűrési feltételként a biztonságintegritási szintet használja, és csak azokat az információkat szolgáltatja, amelyek az elérendő biztonságintegritási szintnél szükségesek, valamint különböző tevékenységeket (pl. életciklus-tervezés) támogató szerkesztőrendszerről.

Az igazán hasznos támogató rendszer a dinamikus funkciók integrálásával jön létre: ezzel egy, az életciklust mindenkor jól követő, azt dokumentáló rendszer kerül a kezünkbe, amely képes a biztonságintegritási szint elérését bizonyító összefoglalók és jelentések automatikus elkészítésére is, így a folyamatok résztvevői, illetve a felelős vezetők folyamatosan képet kapnak a fejlesztés biztonsági vonatkozású megítéléséről. Ez utóbbi funkció azért is kiemelten fontos, mert a külső szakértők és engedélyezők által elvégzendő vizsgálatok alapját képezhetik.

Természetesen az általános, széles körben alkalmazható támogató rendszer alternatíváját képezheti a speciális, adott vállalati informatikai környezetbe illeszkedő támogató rendszer, hiszen jelentős mértékű információigény a vállalati fejlesztő-irányító rendszerekből történő információátvétellel teljesíthető (pl. résztvevők személyi adatai, egyes fázisok eredményei stb.)

6. Összegzés

Cikkünkben összefoglaltuk a biztonságintegritási kritériumokra támaszkodó fejlesztések specifikumait, a kritériumok származtatásának menetét. Kiemeltük a kockázati kritériumok fontosságának, illetve a kockázati alapú gondolkodásnak a szerepét, illetve rávilágítottunk arra a problémára, amely abból származik, hogy a széles fogyasztói közönség, amely az ilyen kritériumok alapján létrehozott rendszerek, pl. járművek vásárlója, illetve üzemeltetője lesz, tájékozatlan a kockázat fogalmát, szerepét illetően, valamint nincs tisztában a kockázatcsökkentés gazdasági vonatkozásaival sem. E területen a szakemberek és a döntéshozók felelősségét hangsúlyoztuk, a döntéshozókét a kockázati alapok melletti elkötelezettség kinyilvánítása területén, a szakemberekét pedig a háttér-információk, ok-okozatok érthető és elfogadható tálalása területén.
Cikkünkben új eredményként javaslatot tettünk egy, a fejlesztést biztonságintegritási szempontból támogató információs rendszer fő funkcióira. Napjainkban a fő funkciók között kiemelt statikus funkciók megvalósítására már léteznek kulcsrakész megoldások, de a dinamikusnak minősített funkciók megvalósítása előrelépésként értékelhető.

Köszönetnyilvánítás

A jelen tanulmány alapjául szolgáló munka részben, illetve a fejlesztés kockázati alapú támogatását elősegítő informatikai rendszer kidolgozása egészében a BME Elektronikus Jármű- és Járműirányítási Tudásközpont (http://www.ejjt.bme.hu/) 5.1 projektjének keretében zajlott, illetve zajlik.

Irodalomjegyzék

[1] MSZ-EN 61508: Finctional safety of electrical/electronic/programmable electronic safety-related systems.

[2] MSZ EN 50126: Vasúti alkalmazások. A megbízhatóság, az üzemkészség, a karbantarthatóság és a biztonság (RAMS) előírása és bizonyítása.

[3] Szabó G. – Tarnai G.: A vasúti biztonság bizonyítására vonatkozó új európai szabványok alkalmazási kérdései. Vezetékek Világa, Magyar Vasúttechnikai Szemle, 2003/1. szám, 2-6 oldal, 2003.

[4] Szabó G. – Szabó K. – Zerényi R.: Safety Management Systems in Transportation: Aims and Solutions. Periodica Politechnica, Ser. Transp. Eng, 2004. Vol. 32. No. 1-2, pp. 123-134.

[5] Szabó G.: Biztonsági terv és kockázatelemzés. MES Sorompó LED optika. Mes Kft. 2005.