Követelmények formalizálásának tapasztalatai a vasúti biztosítóberendezés fejlesztésben

Lukács Gábor* Dr. Bartha Tamás**

Farkas Balázs***

**Budapesti Műszaki és Gazdaságtudományi Egyetem, 1111 Stoczek u. 2. (e-mail: lukacs.gabor@mail.bme.hu).*
***Budapesti Műszaki és Gazdaságtudományi Egyetem, 1111 Stoczek u. 2. (e-mail: bartha.tamas@mail.bme.hu).*
****Budapesti Műszaki és Gazdaságtudományi Egyetem, 1111 Stoczek u. 2. (e-mail: farkas.balazs@outlook.hu).*

Absztrakt: A biztonságkritikus, beágyazott vasúti biztosítóberendezések fejlesztése során alkalmazható formális módszerek gyakorlati alkalmazása egyre inkább a figyelem középpontjába kerül, melynek hátterében a formális módszerek matematikai logikán alapuló, precíz leíró képessége áll. A formális módszerek egyik előnye, hogy alkalmazásukkal jelentősen növelhető a valószínűsége annak, hogy a rendszer formális specifikációja helyes és teljes lesz, melyet például modellellenőrzéssel, mint verifikációs eljárással is megerősíthetünk. Ebben a cikkben összefoglaljuk a fejlesztési életciklus követelményelemzés fázisában történő követelményformalizálással szerzett tapasztalatainkat egy esettanulmány felhasználásával. Bemutatjuk a formalizálás célját, megelőző – előkészítő tevékenységeit, valamint kitérünk a formalizálás egy lehetséges felhasználási módjára a modellvezérelt fejlesztések területén.

1. BEVEZETÉS

A formális módszerek alkalmazása a vasúti biztosítóberendezés fejlesztési terülten nagy múlttal rendelkezik [1 – 4]. Számos elméleti eredményt közlő publikáció jelenik meg [5 – 6], azonban a módszerek és technikák napi szintű mérnöki gyakorlatba való átültetése még várat magára. Az gyakorlati alkalmazási nehézségek mögött számos probléma húzódik, a teljesség igénye nélkül pl. a szükséges háttérismeretek hiánya a szakterületi mérnököknél (két tudományág alkalmazásának az igénye: számítástudomány és közlekedéstudomány), a hagyományos fejlesztési technikákhoz képesti többlet erőforrásigény, az egyszerű rendszerelemek integrációját követően adódó nagyméretű állapotterek kezelésének kérdésköre stb.

Jelen írásunk középpontjába a fejlesztési folyamat követelményelemzés fázisát helyezzük. Bemutatunk egy követelményrendszert és annak egy lehetséges feldolgozási folyamatát. A követelmények előkészítését követően ismertetjük a követelmények formalizálásának módszerét és példákon keresztül mutatjuk be a formalizálással kapcsolatos tapasztalatainkat.

Kutatásunk célja, hogy előkészítsünk egy olyan domain specifikus platformot, amely megteremti a lehetőséget a vasúti szakterületi mérnökök számára – a formális módszerek matematika leírásait elrejtve – a rendszer tulajdonságainak és viselkedésének ellenőrzésére. Jelen írásunkban olyan tapasztalatokat gyűjtöttünk össze, melyek jelentősen hatással lehetnek a platform kialakítására.

1.1. A formális módszerek

A formális módszerek [7] elsősorban az informatika területén használt matematikai (jellemzően diszkrét matematika és matematikai logika) alapú technikák. A formális módszerek támogatják a fejlesztési folyamat egyes tevékenységeit (pl. specifikáció, verifikáció, validáció, stb.) a jól meghatározott szintakszisukkal és szemantikájukkal. A formális módszerek használata biztosítja többek között a helyességet, teljességet, az ellenőrizhetőséget, stb. valamint jó alapot teremt az automatizált feldolgozáshoz is.

A formális módszerek alkalmazása lehetővé teszi az életciklus korai szakaszaiban a hibák detektálását, így azok jelentősen alacsonyabb költségek mellett javíthatóak.

A formális módszerek a rendszertechnikában ismeretes rendszerosztályok (folytonos, diszkrét és hibrid) rendszerek közül kifejezetten a diszkrét (és hibrid rész-) rendszerek kezelésére alkalmasak. A folytonos rendszerekhez képest a diszkrét rendszerek területén a tudományágak teljesen más kihívásokkal küzdenek. Például matematika szempontból folytonos rendszerek esetében az differenciál-, integrál-egyenletek megoldhatósága (pl. megoldást adhat rá a numerikus módszerek alkalmazása), míg diszkrét esetben a nagyméretű állapotterek kezelése (pl. megoldást adhat rá az állapottér csökkentő módszerek használata, pl. ROBDD).

1.2. *Szabványkörnyezet*

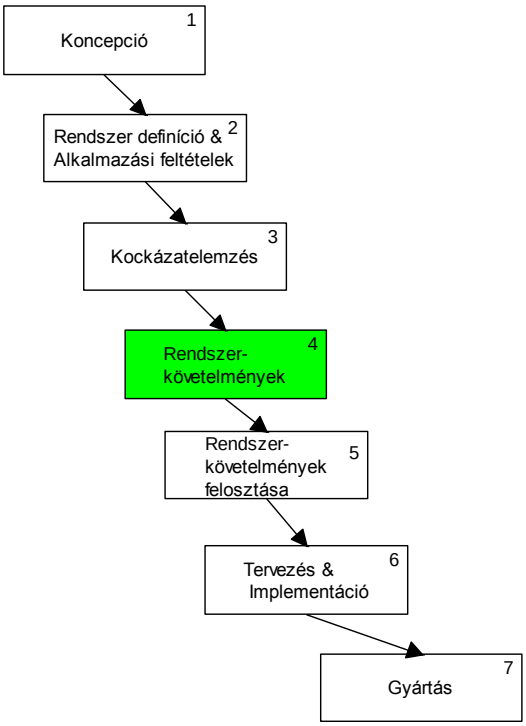
A biztonságkritikus vasúti biztosítóberendezés fejlesztések esetében figyelembe veendő releváns szabványok (elsősorban [9]) is ajánlást tesznek a formális módszerek alkalmazására, például a [9] „A” mellékletet alapul véve:

- A.2 táblázat: SW követelmény-specifikáció,
- A.3 táblázat: SW architektúra,
- A.4 táblázat: SW tervezés és implementáció,
- A.5 táblázat: Verifikációs és tesztelés,
- A.11 táblázat: Adatelőkészítési technikák,
- A.17 táblázat: Modellezés.

[9] szabvány a formális módszereket SIL3-SIL4 biztonságintegritási szinten HR (highly recommended) jelöléssel látja el.

1.3. *Fejlesztési életciklus modell*

A biztonságkritikus vasúti biztosítóberendezés fejlesztések esetében releváns szabványok (pl. [8] és [9]) előírják az fejlesztési életciklus modell megválasztását (ill. definiálását) és alkalmazását, továbbá ajánlást tesznek a V-modell alkalmazására. A [8] szabvány által ajánlott életciklus modell releváns részlete (leszálló ág, 1 – 7 fázisok) az 1. ábrán látható. Az 1. ábrán kiemeltük azt az életciklus fázist, melyet jelen írásunkban középpontba helyezünk.



1. ábra. V-modell, leszálló ág [8.]

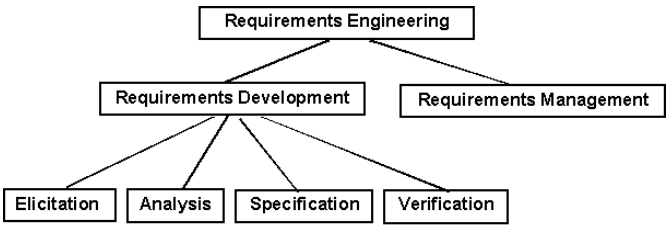
1.4. *Requirement Engineering (RE)*

Egy rendszerfejlesztés kezdetekor végre kell hajtani a követelmények elemzését (Requirements Engineering, RE). Ez az alapvetést manapság szinte már teljesen elfogadottnak tekintik [10 – 13]. A követelményelemzés döntő fontossággal bír a fejlesztési folyamat sikeressége vagy sikertelensége szempontjából. Az RE célja az, hogy eljussunk a homályos kívánalmaktól egy teljes körű, egyértelmű és ellentmondás-mentes követelményhalmazig, amely tükrözi az összes szereplő (stakeholder) konszolidált nézetét. Ez a követelményrendszer képezi a fejlesztés alapját és meglapozza a további fejlesztési tevékenységeket.

Az RE alatt jelen írásunkban a követelményelemzéshez kapcsolódó folyamatot (tudományágat) értjük, beleértve a követelménykezeléshez kapcsolódó folyamatok definiálását, a dokumentációt és karbantartást. Röviden összefoglaljuk az alapvető RE tevékenységeket (2. ábra):

1. *Requirements inception or elicitation (RIE)*
2. *Requirements analysis and negotiation (RAN)*
3. *System modeling (SM)*
4. *Requirements specification (RS)*
5. *Requirements validation (RV)*
6. *Requirements management (RM)*

Megjegyezzük, hogy ezeket az egyértelmű azonosíthatóság miatt angol nevükön adtuk meg.



2. ábra. Az RE összefoglalása [11]

A folyamat a RIE-vel kezdődik, amely tulajdonképpen egy helyzetfelmérés (igényfelmérés) szakasz. Lényege, hogy a fejlesztők és az érdekelt felek találkoznak (előfordulhat, hogy az érdekelt felek előre rögzítik az elvárásaikat, ilyenkor ezt a dokumentumot vitatják meg a fejlesztőkkel). A korszerű fejlesztési módszertanok [14] pedig már a teljes életciklus során ajánlják a felhasználók (mint érdekelt felek bevonását) a fejlesztési folyamatba. A RIE célja, hogy összeálljon egy olyan információ együttes a fejlesztendő rendszerről, melyek alapján meg lehet kezdeni a tényleges fejlesztési munkát.

A RAN célja a követelmények azonosítása és a hozzájuk kapcsolódó esetleges érdekcsoport konfliktusok megoldása. A tevékenység során manapság egyre gyakrabban alkalmaznak valamilyen grafikus rendszerleírásra alkalmas eszközkészletet (pl. UML [15], koncepcionális modell szint) az érdekelt felek és a fejlesztők közötti kommunikáció megkönnyítésére.

Az SM célja, hogy a rendszer felépítését és viselkedését még a megvalósítás előtt megtervezzük és vizsgáljuk. Gyakran a magas szintű felhasználói modelleket egészen az végrehajtási modellekig finomítják.

A rendszerrel szemben támasztott igényeket a követelmény-specifikációban foglalják össze (RS). Sok esetben ez a dokumentum képezi a szerződéskötés alapját is (hiszen pontosan ismerteti a létrehozandó rendszer tulajdonságait, viselkedését és korlátait). Általában mind grafikus, mind szöveges leírást tartalmaz.

Az RV célja, hogy az RS-ben rögzített követelményrendszert különböző szempontok (pl. ellentmondás-mentesség, helyesség, stb.) szerint ellenőrizzük. Az ellenőrzött követelményrendszer ez által válik „hivatalosan elfogadottá”.

Az RM az ellenőrzésen átesett követelményrendszer további életével kapcsolatos tevékenységek kezelésének összefoglaló neve, beleértve pl. a követelmények karbantartását, a változások kezelését, stb. a teljes életciklus alatt.

A vasúti biztonságkritikus rendszerek szoftver fejlesztését részletező [9] szabvány külön szerepkört is dedikál az RE-hez, melyet Requirement Manager (RQM) néven vezet be. A [9] szabvány definiálja az RQM felelősségi körét és a szükséges kulcs kompetenciákat.

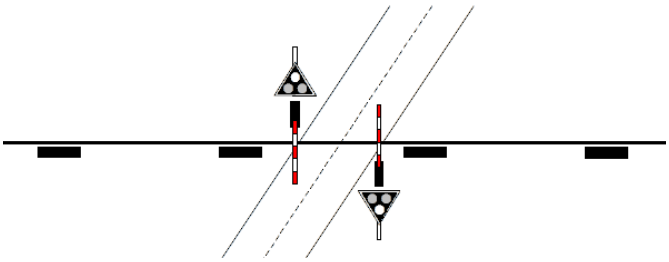
2. ESETTANULMÁNY

A vasúti biztosítóberendezések számos szempont szerint csoportosíthatóak (pl. vonali/állomási, stb.). A biztosító-berendezési szakterületen a rendszerek méretével (bonyolultságával, objektumainak számával) erős korrelációban áll a vonatkozó követelményrendszer mérete is. Az általunk választott esettanulmány egy automata sorompó, amely vonali biztosítóberendezések [16] közül a funkcionalitását tekintve egy közepesen bonyolult rendszernek számít. Az esettanulmányhoz tartozó követelményrendszer tekintetében a gyári követelmény-rendszer (lényegében SR) készítésével és a vonatkozó folyamatokkal nem foglalkozunk (részletesen lásd 2.2. fejezet), így jelen írásunk következő fejezeteiben leírtakat, ezt figyelembe véve kell értelmezni.

2.1. Az elektromos automata sorompó rendszer

A közút-vasút kereszteződések esetében a legbiztonságosabb megoldást a külön szintű keresztezések létesítése jelentené, ami a két közlekedési ág forgalmának teljes szétválasztását jelenti. Azonban külön szintű közút-vasút kereszteződések létesítésére különböző szempontok miatt gyakran nem adódik lehetőség (pl. költségek, stb.). Amennyiben indokolttá válik – pl. számottevő közúti forgalomnagyság, nagy sebességű vasútvonal, stb. – a közút-vasút szintbeni kereszteződést (jellemzően új telepítés esetében) elektronikus automata sorompóval (későbbiekben sorompó-berendezés) biztosítják.

A sorompó-berendezés egy lehetséges kiépítésére láthatunk példát a 3. ábrán. A közút számára 2 fénysorompó és két félsorompó ad jelzést, melyek működését a vasúti pályára telepített érzékelőelemek felett elhaladó vonatok kezdeményezik.



3. ábra. Sorompó-berendezés vázlat egy lehetséges konfigurációval

Megjegyezzük, hogy létezik olyan konfiguráció is, melyben a vasúti közlekedési irány is kap jelzéseket (pl. fedezőjelző) a fény- és félsorompó állapotáról.

2.2. A követelményrendszer bemutatása

Ha egy sorompó-berendezés fejlesztésébe fogunk, akkor számos követelményforrással kell számolnunk. Ezek egy részére hierarchiát is definiáltak, a következő listában a lista elején lévő követelményforrások képezik a hierarchia csúcsát (megjegyezzük, hogy lenti felsorolás nem teljes körű, valamint nem minden esetben definiált egyértelműen a hierarchia, vagy egyszerűen értelme sincs definiálni). Az egyértelműen definiált hierarchia szinteket + jellel jeleztük [17 – 18]:

+ EU jog (elsődleges jog, nemzetközi megállapodások, rendeletek, határozatok, ajánlások, vélemények),

+ magyar jog (alaptörvény, törvény, kormányrendelet, miniszterelnöki rendelet, miniszteri rendelet, önkormányzati rendelet),

- Vállalati (üzemeltetői) szabályozás (utasítás, feltétfüzet, műszaki előírás, vállalati szabvány, stb.)

- Gyártói követelmények

- Tervezői követelmények

- Szabványok (EN, MSZ EN, ISO stb.)

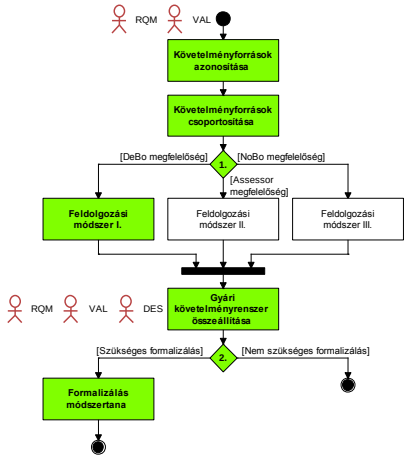
- Stb.

Jelen bekezdésben összefoglalunk néhány olyan szempontot, mely jól jellemzi a sorompó-berendezés fejlesztésben releváns követelményrendszer tulajdonságait. A fenti listában szereplő követelményforrások rendkívül heterogének, sok esetben teljesen különböző feldolgozási módot igényelnek. A követelményforrások követelményei gyakran teljesen más szintű követelményeket közölnek, melyek lebontása nem egyértelmű, még tapasztalt követelménymenedzserek is félreértelmezhetik azokat. Pl. az egyes fogalmak a legtöbb esetben csak az adott joganyag értelmezése szerint és csak az adott joganyagra érvényesek. Nagyon fontos a követelmény szövegkörnyezete is, amely komoly hatást gyakorolhat a követelmény értelmezésére. A követelményforrások gyakran ellentmondásos követelményeket támasztanak (sok esetben önellentmondásról is beszélhetünk), melyek tisztázása rendkívül körülményes lehet. A követelményforrások legtöbbje általában az életciklus legtöbb fázisára vonatkozóan tartalmaz előírásokat, melyek közvetetten visszahathatnak a fejlesztésre.

A következő fejezetekben nem foglalkozunk a gyártói követelményekkel (a gyártói követelményrendszer összeállításával), a szabványokkal, a tervező által meghatározott követelményekkel, valamint az EU-s jogrendből származó követelményekkel. Ezeket figyelmen kívül hagyva a megmaradó követelményrendszerhez kapcsolódóan néhány statisztikai adat: összesen 27 feldolgozott követelményforrás (67 azonosított követelmény-forrásból), 2588 tisztázott követelmény, amiből 1487 formalizálható. Megjegyezzük, hogy a követelményforrások feldolgozás jelenleg is tart.

3. A KÖVETELMÉNYFORMALIZÁLÁST ELŐKÉSZÍTŐ FOLYAMATOK

A követelmények feldolgozásának összefoglaló folyamatábráját a 4. ábrán láthatjuk. A 2.2. fejezetben leírtak alapján zöld színnel jelöltük azt a folyamatábra részt, melyet jelen írásunkban részletesen bemutatunk.



4. ábra. Követelmény feldolgozás, összefoglalás

3.1. A követelményforrások azonosítása

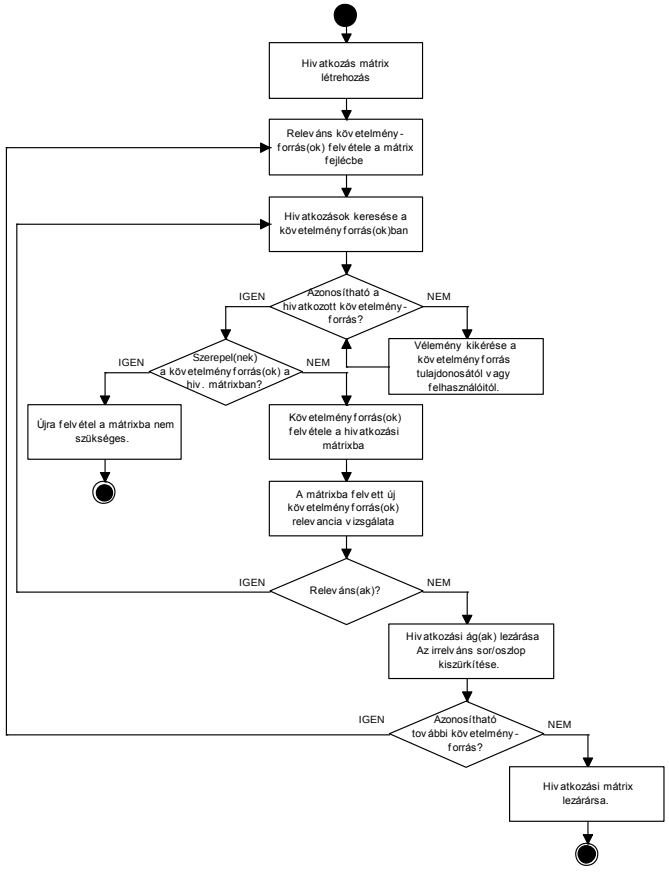
A gyakorlatban a releváns követelményforrások azonosítása általában a rendszerfejlesztést végző szakterületi mérnökök feladata, akik korábbi tapasztalataikra építve, egzakt módszer felhasználása nélkül végzik el ezt a tevékenységet. A következőkben felsorolunk néhány olyan követelményforrás keresési platformot, melyek elősegítik a releváns követelményforrások tekintetében a teljesség elérésének lehető legjobb megközelítését (a vasúti biztosítóberendezés fejlesztésekben):

- korábban fejlesztett hasonló rendszerek azonosított követelményforrásainak vizsgálata,
- a gyártó cég követelményforrás gyűjteményének áttekintése,
- kulcsszavakra való keresés bármilyen fórumon (pl. interneten, joganyagok (net.jogtar.hu), szabványok (mszt.hu), EU-s szabályozás (http://eur-lex.europa.eu),
- a fejlesztés stratégia és koncepció fázisában előállított dokumentumok áttekintése (pl. utalhatnak a fejlesztés által megcélzott területre, országra, így az adott ország vonatkozó joganyagait, az ott lévő üzemeltetők előírásait stb. is fel kell dolgozni,
- - a fejlesztésben résztvevő mérnökök korábbi tapasztalati alapján ismert követelményforrások összegyűjtése,
- bármilyen a rendszerrel közvetetten vagy közvetlenül kapcsolatban lévő személy véleményének kikérése (pl. üzemeltető, tanúsító, hatóság stb.),
- üzemeltetői követelményforrások átvizsgálása (pl. utasítások, feltétfüzetek stb.),
- tervező által készített korábbi tervek átvizsgálása,
- Stb.

Előbbiekben áttekintettünk egy olyan releváns követelmény-forrás azonosítási módszert, mely elterjedten alkalmazott a gyakorlatban, ugyanakkor erősen tapasztalati. A következőkben bemutatunk egy olyan, a fejlesztéshez releváns követelményforrások azonosítására vonatkozó módszert, amely fent ismertetett tapasztalati módszerhez képest lehetővé teszi a releváns követelményforrások teljes körű levezetését megadott határparaméterek mellett. Ez módszer akár validációs ill. verifikációs (V&V) technikaként is alkalmazható.

A releváns követelményforrások teljeskörű azonosítását megcélzó módszer egy mátrixra épül, amit hivatkozási mátrixnak neveztünk el. A módszer bemenete a szakterületi mérnök által megadott releváns követelményforrásokat összefoglaló lista (megjegyezzük, hogy elegendő, ha ez a lista mindössze egyetlen elemből áll, pl. a sorompó-berendezés esetében [19]). A módszer lényege, hogy a megadott követelményforrásokból kigyűjti az összes az adott

dokumentumból kifelé mutató hivatkozást és vizsgálja azokat relevancia szempontjából. A folyamat lényeges elemeit az 5. ábrán mutatjuk be.



5. ábra. Hivatkozási mátrix kezelése

3.2. A követelményforrások csoportosítás

A fejlesztett vasúti biztosítóberendezések esetében a megfelelőséget három szervezet vizsgálhatja:

- DeBo,
- NoBo,
- Assessor.

Mindhárom szervezet esetében más célok állnak a vizsgálat középpontjában:

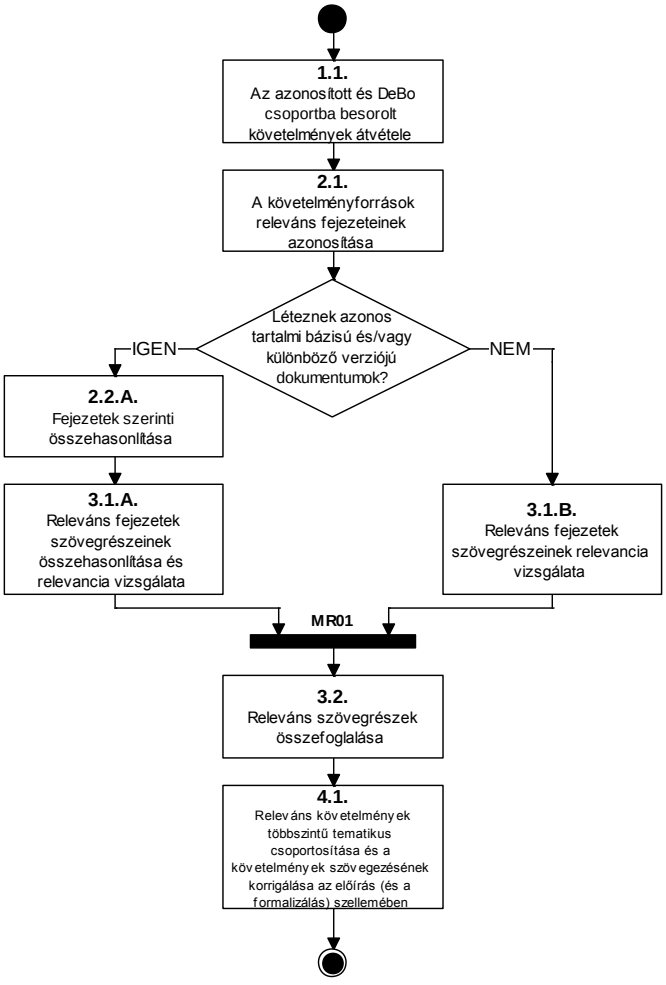
- DeBo: a nemzeti követelményeknek való megfelelőséget vizsgálja (törvények, rendeletek stb. Ezen kívül ide értjük az üzemeltető, mint szervezet követelményeit is (feltétfüzet, utasítás stb.),
- NoBo: az átjárhatósági előírásoknak való megfelelőséget vizsgálja (pl. TSI/ÁME),
- - Assessor: a szabványoknak való megfelelőséget vizsgálja (pl. EN 50126 stb.).

Célszerű már a követelményforrások azonosításakor megállapítani (a legtöbb esetben ez külön vizsgálat nélkül megtehető), hogy melyik vizsgálati célhoz tartozik majd a követelményforrás.

A csoportosítást követően elérjük a követelmény-feldolgozási folyamatunk 1. mérföldkövét (lásd 4. ábra, rombusz). A folyamatunk itt a megfelelőség vizsgálat függvényében három ágra szakad, mely ágak közül jelen írásunkban részletesebben a „Feldolgozási módszer I.” ágat ismertetjük részletesebben (A választás oka mögött az áll, hogy ezen a szinten megfogalmazott követelmények már kellően alacsony szintűek (részletekbe menőek) a közvetlen formalizáláshoz, lásd. 2.2. fejezet, a követelmények több mint fele formalizálható volt).

3.3. Feldolgozási módszer a nemzeti követelményeknek való megfelelőség vizsgálatához

A módszer egyszerűsített lépéseit a 6. ábrán szemléltetjük.



6. ábra. Követelmény-feldolgozási módszer I.

A 4. ábrán jelzett 2. mérföldkövet megelőzi a fejlesztés egyik alapvető dokumentumának, a gyári követelmény specifikációnak az elkészítése. Az esettanulmányban ezt a

lépést kihagytuk (lásd. 2.2. fejezet) azért, mert az esettanulmány során nem tűztük ki célul a teljes gyári követelmény rendszer összeállítását (annak rendkívüli erőforrás igényei miatt).

A 4. ábrán jelzett 2. mérföldkő elérésekor a fejlesztés korábbi szakaszaiban előírtaknak megfelelően döntünk a követelményformalizálás – általánosabban a formális módszerek, mint technikáknak – alkalmazásáról. Külön nem részletezzük [9] erre vonatkozó ajánlásait az alkalmazott technikák kiválasztásáról, SIL szintről, stb. Például az sorompó-berendezés esetében, amely hazánkban egy SIL4 funkciókból álló biztonsági berendezés [9] A.2 táblázata alapján egy lehetséges választható kombináció a formális módszerek melletti természetes nyelven leírt követelmény specifikáció (a természetes nyelvű leírás kötelező elem).

4. KÖVETELMÉNYFORMALIZÁLÁS

A követelmények formalizálásának igénye a fejlesztési tapasztalatok alapján keletkezett, hiszen számos hiba a hiányos vagy ellentmondásos követelményspecifikációra vezethető vissza [19]. Megoldást jelenthet erre a szigorú specifikációs nyelvek használata, ellenőrzött tervezési minták készítése és a specifikáció ellenőrzése [20]. Jelen írásunkban utóbbit tűztük ki célul (lásd 4.5. fejezet).

4.1. A CTL nyelv

A formális nyelvek közül a követelmények formalizálása céljából a CTL (Computational Tree Logic) nyelvet választottuk, mert a formalizált követelményeket modell-ellenőrzésre szeretnénk felhasználni (és a modellellenőrzés általunk kiválasztott eszközök egy része is ezt a nyelvet támogatja), továbbá a CTL nyelv kellően egyszerű a vasúti szakterületi alkalmazásokhoz [22 – 23]. A CTL nyelv az elágazó idejű temporális logikák csoportjába tartozik. A CTL nyelv részletekbe menő ismertetésére külön nem térünk ki, jó leírást olvashatunk róla például [21]-ben.

4.2. Követelmények formalizálhatósága

Az esettanulmány követelményei a formalizálhatóság szempontjából három csoportra bontottuk:

- Formalizálható követelmények: melyek egyértelműen leírhatóak CTL nyelv segítségével,
- Nem formalizálható követelmények: melyek nem írhatóak le CTL nyelvvel,
- Modellfüggő a követelmény formalizálhatósága: a követelmények formalizálása jelentősen függ a modelltől (pl. annak részletezettségétől).

A következő alfejezetekben mindhárom csoportra mutatunk be példákat felhasználva a 3. fejezetben bemutatott esettanulmány.

4.3. Példa egy követelmény formalizálására

1. táblázat. Az eredeti követelmény

Követelmén-azonosító	Követelmény szövege	Formalizálható?
UT4-132-003-01	A késleltető szerkezet a berendezést az előírt idő letelte után szükség esetén lekapcsolja.	igen

2. táblázat. Formalizálásra előkészített követelmény

CTL operátor	HA	Kifejezés	AKKOR	Kifejezés	Modellellenőrzés elvárt eredménye
EF	-	(berendezés lekapcsolási időzítés indul)	-	-	TRUE
AG	+	(berendezés lekapcsolási időzítés lejár)	+	(a berendezés lekapcsol)	TRUE

Az 1. és 2. táblázatok alapján látható az a gyakori jelenség, hogy egy természetes nyelven megfogalmazott követelmény több követelményre esik szét a formalizálás során (Természetesen ez nagyban függ az atomi kijelentések célszerű megválasztásától).

A formalizált követelményt nem ismertetjük, mert a vonatkozó modellrész még fejlesztés alatt áll. A formalizált követelmény erősen függhet a modelltől (pl. változónevek), ill. függ az alkalmazott modellellenőrző szintaktikájától esetleg szemantikájától.

4.4. Példák nem formalizálható követelményekre

3. táblázat. Nem formalizálható követelmény, 1. példa

Követelmén-azonosító	Követelmény szövege	Formalizálható?
FF7-129-030-00	prEN 50129 Vasúti alkalmazások: Biztonságorientált elektronikus rendszerek.	nem

A 3. táblázatban szereplő követelmény egy hivatkozás: nem formalizálható.

4. táblázat. Nem formalizálható követelmény, 2. példa

Követelmén-azonosító	Követelmény szövege	Formalizálható?
FF7-166-019-00	A karbantartási utasításban meg kell határozni, hogy mi a forgalmi kezelőszemélyzet teendője a zavarok, illetve meghibásodások esetén.	nem

A 4. táblázatban szereplő követelmény egy dokumentációra vonatkozó követelmény: nem formalizálható.

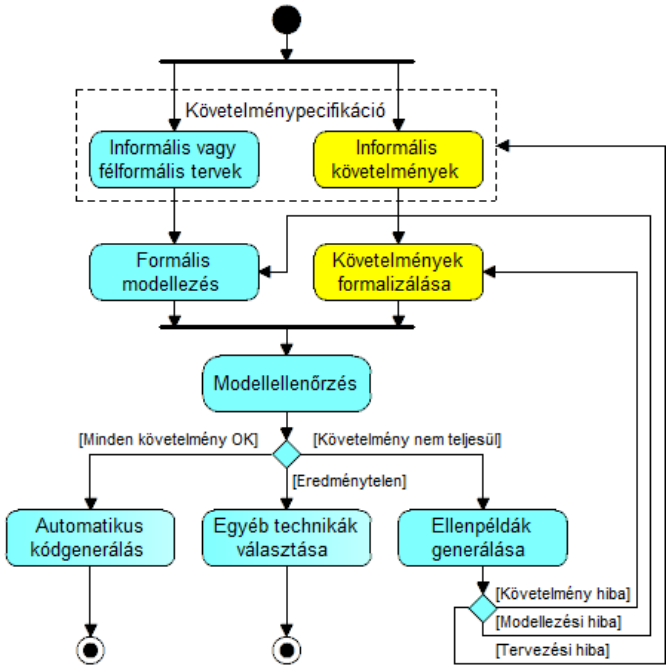
5. táblázat. Modellfüggő a követelmény formalizálhatósága, 3. példa

Követelmén-azonosító	Követelmény szövege	Formalizálható?
JSZ2-065-002-00	Rendkívüli esemény: A vasút területén bekövetkezett minden olyan zavar vagy akadály, amely a vonatközlekedést kizárja, akadályozza vagy jelentős forgalmi zavart okoz.	Jelentősen függ a modelltől

Az 5. táblázatban szereplő követelmény egy fogalom: formalizálhatósága jelentősen függ a modelltől. Ezen követelmények formalizálásnak előkészítését a modellezési cél meghatározásáig nem hajtjuk végre.

4.5. *A formalizált követelmények egy lehetséges felhasználása: a modellellenőrzés*

A formalizált követelmények egy lehetséges felhasználását, a modellellenőrzést mutatja be a 7. ábra [21-23].



7. ábra. Formalizált követelmények egy lehetséges felhasználása

A modellellenőrzés [21] egy olyan formális módszer, amely a vizsgálandó rendszer egy modelljéről (viselkedés leírás) és annak elvárt működését tartalmazó követelmény-specifikációjáról (tulajdonság leírás) a rendszermodell teljes állapotterének szisztematikus bejárásával dönti el, hogy a rendszermodell a követelmény- specifikációt teljesíti-e vagy sem. A modellellenőrzés kimenete (a felhasznált modellellenőrző eszköztől függően) a vizsgált követelmény nem teljesítése esetében egy ellenpélda.

5. TAPASZTALATOK ÖSSZEFOGLALÁSA

5.1. *A követelményformalizálást előkészítő tevékenységekkel szerzett tapasztalatok*

A követelmények formalizálását előkészítő folyamat rendkívül erőforrás-igényes, monoton munkavégzést igénylő tevékenységsorozat. A folyamat hatékonysága növelhető követelmény-adatbázisok szervezésével, ill. egy célszerűen megválasztott CASE eszköz alkalmazásba vételével, azonban a megfelelő CASE eszköz kiválasztás a sok választási szempont (pl. nyomonkövetés, verziókövetés, nézetek, csoportosítás, hierarchikus felépítés, relációk kezelése, stb.) miatt nehézkes lehet.

A releváns követelményforrások azonosítására bemutattunk egy használható, egzakt módszert (hivatkozás mátrix), azonban a mátrix előállítása rendkívül erőforrás igényes lehet nagyobb követelményrendszerek esetében. A mátrix előállítását nagyban nehezítik a pontatlan hivatkozások, ill. hogy a nyomonkövethetőség nem minden esetben egyértelmű. A módszer alkalmas a szakterületi mérnökök által adhoc módon végzett követelményforrás azonosítás verifikációjára.

5.2. *A követelményformalizálásban szerzett tapasztalatok*

A formalizálás bemenetét képező természetes nyelvű követelményspecifikáció a formalizálás segítségével hatékonyan javítható (kivételt képeznek ez alól a hiányosságok). A formalizálás segíti a követelményrendszer nehézségeinek (pl. ellentmondások) a megoldását.

A modellezés – mely jelen írásunkban csak érintőlegesen a modellellenőrzés kapcsán érintettünk – jelentős hatással van a követelmények formalizálására pl. többek között ide értendő a modellezés célja.

A formalizálást előkészítő lépésiben a követelmények még természetes nyelven is jól olvashatóak maradnak, a formalizálást követően azonban már csak matematika jelek sokasága. Érdekes kérdést vet fel ezzel kapcsolatban, hogy pl. a modellellenőrzés során feltárt ellenpélda milyen módon forgatható vissza természetes nyelvre, hogy a vasúti szakterületi mérnökök is megértsék a hibát.

Az eddigi tapasztalataink alapján megállapítjuk, hogy a követelmények formalizáláshoz szükség van vasúti szakterületi mérnök közreműködésére a következőkben:

- Félreértések elkerülése: pl. a kifejezések konstruálásakor jelentős tartalmi különbségek léphetnek fel az eredeti megfogalmazáshoz képest,
- Döntési helyzetek felelőssége: pl. hasonló tartalmú kifejezések összevonása,
- Követelmények célszerű felbontása: pl. egy követelményből a formalizálás során több követelmény létrehozásának szükségessége,

– Temporális logika ismerete: a követelmények a legtöbb esetben még csak utalást sem tesznek a használandó operátorokra.

6. ÖSSZEFOGLALÁS

Jelen írásunkban bemutattuk a vasúti biztosítóberendezések fejlesztésének követelményelemzési fázisával kapcsolatos problémaköröket és a követelmények feldolgozásának egy lehetséges módját (folyamatát). Egy célszerű esettanulmányból kiragadott példák segítségével ismertettük a követelmények formalizálásnak előkészítését, bemutattuk a formalizált követelmények egy lehetséges gyakorlati alkalmazását, a modellellenőrzést. Összefoglaltuk a formalizálást előkészítő folyamatokkal kapcsolatos tapasztalatainkat.

Kutatásunk célja közt van, hogy létrehozzunk egy olyan domain specifikus platformot, amely megteremeti a lehetőséget a vasúti szakterületi mérnökök számára a formális módszerek matematika leírásait elrejtve a rendszer tulajdonságainak és viselkedésének ellenőrzését. Jelen írásunkban olyan tapasztalatokat gyűjtöttünk össze, melyek jelentősen befolyásolhatják a platform kialakítását.

7. HIVATKOZÁSOK

[1] Sághi B. Formális módszerek alkalmazása a vasútbiztosító technikában, PhD értekezés, Budapest, 2003.

[2] A. Cimatti, et al. Formal Verification of a Railway Interlocking System using Model Checking, Formal Aspects of Computing, Vol. 10, Issue 4., pp 361-380, 1998.

[3] Arne B. Case Study: Formal Verification of a Computerized Railway Interlocking, Formal Aspects of Computing, Vol. 10, Issue 4, pp 361-360, 1998.

[4] M. Banci, et al. The Role of Formal Methods in Developing a Distributed Railway Interlocking system, http://fmt.isti.cnr.it/webpaper/forms_04.pdf

[5] L. H. Vu, et al. Formal modeling and verification of interlocking systems featuring sequential release, Science of Computer Programming, Vol. 133, Part 2, pp. 91-115, 2017.

[6] A. Bonacchi, et al. Validation of Railway Interlocking Systems by Formal Verification, A Case Study, Internal Conference on Software Engineering and Fornmal Methods, pp 237-252, 2013.

[7] Pataricza A., et al. Formális módszerek az informatikában, ISBN 978-963-9548-90-9, 2006.

[8] MSZ EN 50126:2001 Vasúti alkalmazások. A megbízhatóság, üzemkészség, a karbantarthatóság és a biztonság (RAMS) előírásai és bizonyítása. 1. rész: Alapvető követelmények és az általános folyamat.

[9] MSZ EN 50128:2011 Vasúti alkalmazások. Távközlési, biztosítóberendezési és adatfeldolgozó rendszerek. Szoftverek vasúti vezérlő- és védelmi rendszerekhez

[10] I. SOMMERVILLE, P. SAWYER, REQUIREMENTS ENGINEERING: A GOOD PRACTICE GUIDE (WILEY, 1997)

[11] KARL E. WIEGERS WHEN TELAPTAHY WON’T DO: REQUIREMENTS ENGINERRING KEY PRACTICES

[12] B. Nuseibeh, S. Easterbrook: Requirements Engineering: A Roadmap, 2000

[13] A. v. Lamsweerde: Formal Specification: a Roadmap, 2000

[14] Manifesto for Agile Software Development, 2001 http://agilemanifesto.org/

[15] Unified Modeling Language, http://www.omg.org/spec/UML/

[16] Németh L.Vonali biztosítóberendezések, MÁV Rt. Vezérigazgatóság, 2000.

[17] Magyarország Alaptörvénye (2011. Április 25.), https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100425.ATV

[18] Az Európai Uniós jog forrásai és hatálya, 2017. http://www.europarl.europa.eu/ftu/pdf/hu/FTU_1.2.1.pdf

[19] Dávid I.Az űrhajózás történetének legnagyobb katasztrófái, 2015. http://24.hu/tudomany/2015/05/09/az-urhajozas-tortenetenek-legnagyobb-katasztrofai/

[20] Majzik I. Követelmény-specifikáció készítés és ellenőrzés, 2016.

[21] Ésik Z. [et al.] Hardver- és szoftverrendszerek verifikációja, Typotex, 2011, ISBN 978-963-279-497-6, http://www.tankonyvtar.hu/hu/tartalom/tamop425/0008_esikgombasnemeth/Esik_Gombas_Nemeth_Hardver_1_1.html

[22] Farkas B., Lukács G., Dr. Bartha T. Formális modellezés alkalmazásának lehetőségei a vasúti biztosítóberendezések területén – 1. rész, Vasúti vezetékvilág XXII. 2017/2

[23] Farkas B., Lukács G., Dr. Bartha T. Formális modellezés alkalmazásának lehetőségei a vasúti biztosítóberendezések területén – 2. rész, Vasúti vezetékvilág XXII. 2017/3