FEJLESZTÉSI FOLYAMATOK ONTOLÓGIA ALAPÚ ELLENŐRZÉSE

Szatmári Zoltán

Abstract
Our everyday life depends on software to a considerable extent, this way the reduction of the risks of design and implementation faults is of utmost importance. Software development processes are more and more subject to regulations fixed in standards that define criteria for the selection of proper development methods. The goal of this work is to support the assessment of development processes and toolchains by elaborating a formal verification technique that allows the automated checking of the compliance to standards.

Key words:
Safety critical systems, process modeling, ontology, reasoning, model transformation, standard based assessment

Összefoglalás
Mindennapi életünk jelentős mértékben függ a szoftverektől, így egyre fontosabbá válik a szoftver tervezési és implementációs hibákból adódó kockázatok csökkentése. A különféle szabványok egyre inkább szabályozzák a szoftverfejlesztési folyamatokat, többek között kritériumokat fogalmaznak meg az alkalmazandó fejlesztési módszerek kiválasztására. Ezen munkám célja, hogy formális verifikációs technikák felhasználásával elősegítsem a fejlesztési folyamatok értékelését a szabványoknak való megfelelőség szempontjából.

Kulcsszavak:
Biztonságkritikus rendszerek, folyamatmodellezés, ontológia, következtetés, modell transzformáció

1. Bevezetés

Biztonságkritikus alkalmazási környezetbe történő szoftverfejlesztés esetén kiemelten fontos a vonatkozó fejlesztési szabványokban található követelmények betartása. Annak igazolásához, hogy a fejlesztési folyamat ténylegesen megfelel a vonatkozó szabványok előírásainak, független és külső értékelés szükséges. A megfelelőség ellenőrzésére, az értékelő munkájának támogatására modell alapú verifikációs technikákat javaslunk: a fejlesztési folyamatot és eszközöket egy ontológia alapú folyamatmodell segítségével írjuk le, és logikai következtető segítségével ellenőrizzük a szabvány szerinti követelmények teljesülését.

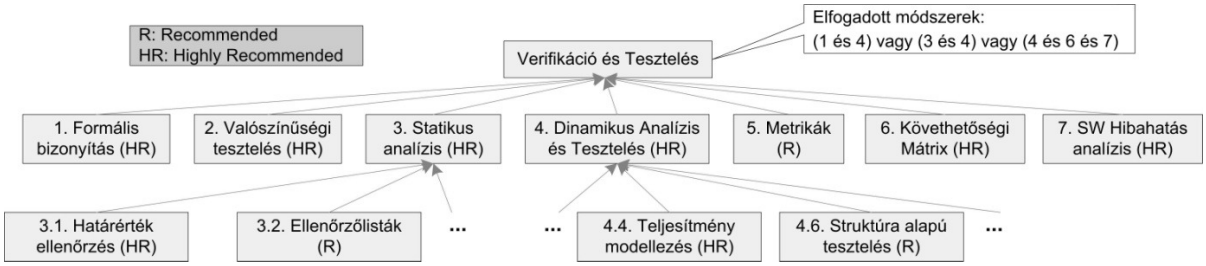
2. Követelmények formalizálása

A fejlesztési folyamatok formális verifikációjának előfeltétele a követelmények formális leírása. Munkám során biztonságkritikus beágyazott szoftverek fejlesztési folyamatainak szabványait

vizsgáltam meg, ezen belül példaként az EN50128-as szabványt hivatkozom, ami vasúti vezérlő- és ellenőrzőrendszerekhez készülő szoftverek fejlesztését szabályozza [1].

A szabvány öt különböző biztonságintegritási szintet (Safety Integrity Level - SIL) definiál a fejlesztési folyamatok számára és előírja azon módszereket, melyek a folyamatok során alkalmazandóak. Mindegyik fejlesztési lépéshez táblázatos formában megadja, hogy annak során az egyes módszereket kötelező (mandatory – M), erősen ajánlott (highly recommended – HR), ajánlott (recommended – R), vagy nem ajánlott (not recommended – NR) alkalmazni.

A követelményformalizálás több fontos kihívást is tartalmaz. A fejlesztési módszerek hierarchikusan finomíthatóak, azaz egyes magasabb szintű módszerek felbonthatóak több (alternatív) alacsonyabb szintű módszer kombinációjára (lásd 1. ábra).



1. ábra. *A verifikációs és tesztelési módszerek hierarchikus finomítása (EN50128)*

A szabvány a különböző SIL szintekhez különböző követelményeket fogalmaz meg, mely egy újabb dimenziót vezet be a formális leírásba (lásd 1. táblázat). Végső soron az alkalmazott módszerek különböző kombinációi alapján elégséges feltételeket találhatunk minden egyes SIL szint eléréséhez.

1. táblázat. *Verifikációs és tesztelési módszerek*

Módszer	SIL1	SIL2	SIL3	SIL4
1. Formális bizonyítás	R	R	HR	HR
2. Valószínűségi tesztelés	R	R	HR	HR
3. Statikus analízis	HR	HR	HR	HR
4. Dinamikus analízis és tesztelés	HR	HR	HR	HR
5. Metrikák	R	R	R	R
6. Követhetőségi mátrix	R	R	HR	HR
7. SW hibahatás analízis	R	R	HR	HR

A fent ismertetett jellemzőkkel rendelkező követelmények formalizálására célszerű ontológia alapú leírást alkalmazni, mert az ontológiák alkalmasak hierarchikus fogalmi struktúrák és logikai kifejezések modellezésére.

Az ontológiák széles körben alkalmazott nyelvek, melyek segítségével egy adott szakterület fogalmai és a köztük lévő kapcsolatok leírhatók. Mindezek mellett az ontológiákhoz kapcsolódó hatékony logikai következtető algoritmusok segítségével lehetőség van többek között a logikai kifejezések kiértékelésére is.

3. Fejlesztési folyamatok modellezése

Fejlesztési folyamatok leírására az OMG (Object Management Group) által javasolt SPEM (Software Process Engineering Metamodel) alapú leírást használom, hiszen ez kifejezetten fejlesztési folyamatok modellezését tűzi ki célul. Ehhez egy megfelelő és ingyenes eszköz is rendelkezésre áll, hogy a fejlesztőmérnökök a folyamatmodelljeiket elkészítsék. Ahhoz, hogy ontológia alapú verifikációs technikát tudjunk alkalmazni, szükséges, hogy magát a fejlesztési folyamatot ontológia alapú formalizmussal írjuk le. Ezen formalizmus alapjául a W3C által készített OWL-S [2,3] szabvány szolgál, ami többek között fejlesztési folyamatok ontológia alapú leírását támogatja.

Az OWL-S ontológia definiálja a „Process" fogalmat, amit „Atomic Process" vagy „Composite Process" diszjunkt halmazokra bonthatunk fel. Az „Atomic Process" fogalom reprezentálja az elemi lépéseket, míg a „Composite Process" az összetett folyamatstruktúrákat (mint például az elágazás, ciklus, vagy sorrendi végrehajtás) írja le. Minden vezérlési struktúra elemei újra „Process" típusú egyedek lesznek, így rekurzív módszerrel definiálhatóak a fejlesztési folyamatok.

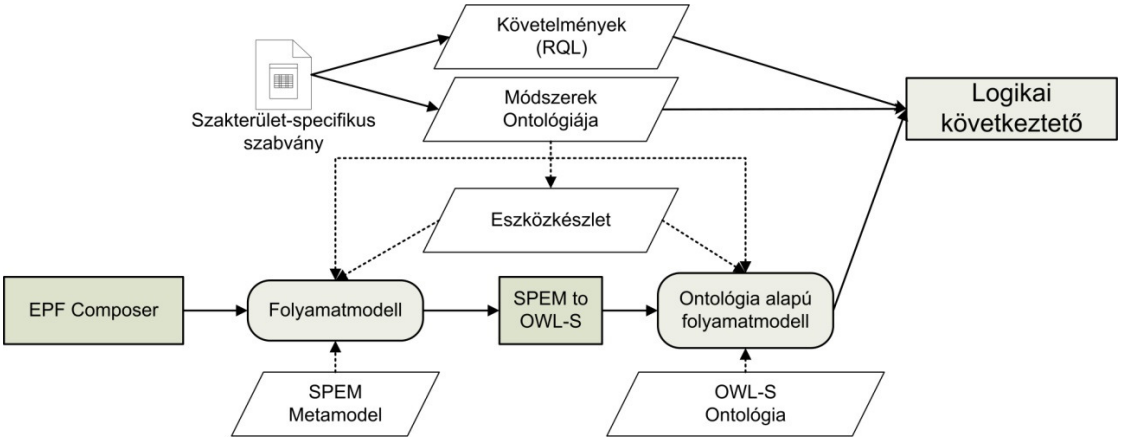
A fejlesztési folyamat egyes lépései valósítják meg a szabványban leírt módszereket. A módszerek osztályozása szolgál alapul a fejlesztési folyamat értékeléséhez: a szabványban foglalt módszerek hierarchiájának leírásához elkészítettem a „módszerek ontológiáját" az OWL-S ontológia kiegészítéseként. Az OWL-S által definiált „Process" fogalom hierarchikus finomítása során vezettem be a különböző módszereket ábrázoló fogalmakat.

Az ontológia alapú ábrázoláshoz a SPEM metamodell szerint elkészített folyamatmodelleket OWL-S struktúrába kell transzformálni. Mindkét folyamatreprezentáció XML alapú leírással rendelkezik, ezért egy XSLT transzformáció segítségével oldottam meg SPEM modell OWL-S modellbe való leképzését.

4. Az értékelés folyamata

A fejlesztési folyamatok értékelését egy eszközkészlet segítségével valósítottam meg (lásd 2. ábra), mely biztosítja a fejlesztők számára, hogy a bemeneti modellen automatikusan végrehajthatóak legyenek az értékeléshez szükséges különböző lépések.

Első lépésként a fejlesztő előállítja a folyamat modelljét az EPF Composer alkalmazással, ami támogatja SPEM folyamatmodellek létrehozását. Ezen modellben foglalt elemi lépések felcímkézésre kerülnek a szabványba foglalt módszerek típusával. Az elkészített bemeneti folyamatmodell ontológia alapú (az OWL-S és a „módszerek ontológiája" által definiált) modellé való automatikus transzformációja után a logikai következtető segítségével van lehetőség a szabványban található követelmények ellenőrzésére.



2. ábra. *Az értékelés folyamata*

A szabványban található követelmények, az egyes módszerek ajánlott vagy éppen nem ajánlott volta és az elégséges feltételek mint logikai kifejezések fogalmazhatóak meg az RQL lekérdező nyelven. A fejlesztési folyamat követelményeknek való megfeleléséhez valamelyik elégséges feltételt ki kell elégíteni, de egyik nem ajánlott módszert sem szabad használni.

5. Összefoglalás

A dolgozatomban bemutattam, hogyan lehet a fejlesztési folyamatokra vonatkozó szabványokban meghatározott követelmények ellenőrzését ontológiai következtetők segítségével megvalósítani. A bemutatott eszközkészlet lehetőséget biztosít a fejlesztő mérnökök és értékelők számára, hogy a használt fejlesztési folyamatok szabványnak való megfelelőségét megvizsgálják.

Irodalom

[1] CENELEC, „En 50128: Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems” URL: http://www.cenelec.eu.

[2] P. M. Anupriya, A. Ankolekar, M. Paolucci, and K. Sycara, “Towards a formal verification of OWL-S” in In Fourth International Semantic Web Conference (ISWC 2005).

[3] J. Shen, Y. Yang, C. Wan, and C. Zhu, “From BPEL4WS to OWL-S: Integrating e-business process descriptions” in Proc. IEEE International Conference on Services Computing (SCC’05), pp. 181–190, Washington DC, USA, 2005. IEEE Computer Society.

Szatmári Zoltán, doktorandusz

Budapesti Műszaki és Gazdaságtudományi Egyetem, Villamosmérnöki és Informatikai Kar,

Méréstechnika és Információs Rendszerek Tanszék

H-1117, Magyarország, Budapest, Magyar tudósok krt. 2.

Tel: +36-1-463-3579, E-mail: szatmari@mit.bme.hu