FELADATKIÍRÁS

A feladatkiírást a tanszéki adminisztrációban lehet átvenni, és a leadott munkába eredeti, tanszéki pecséttel ellátott és a tanszékvezető által aláírt lapot kell belefűzni (ezen oldal *helyett*, ez az oldal csak útmutatás). Az elektronikusan feltöltött dolgozatban már nem kell beleszerkeszteni ezt a feladatkiírást.

Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Méréstechnika és Információs Rendszerek Tanszék

Modellelemek effektív jogosultságainak származtatása finomszemcsés hozzáférési szabályokból

Szakdolgozat

Készítette
Balogh Tímea

Konzulens
Debreceni Csaba

2017. november 23.

Tartalomjegyzék

HALLGATÓI NYILATKOZAT

Alulírott *Balogh Tímea*, szigorló hallgató kijelentem, hogy ezt a szakdolgozatot meg nem engedett segítség nélkül, saját magam készítettem, csak a megadott forrásokat (szakirodalom, eszközök stb.) használtam fel. Minden olyan részt, melyet szó szerint, vagy azonos értelemben, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

Hozzájárulok, hogy a jelen munkám alapadatait (szerző(k), cím, angol és magyar nyelvű tartalmi kivonat, készítés éve, konzulens(ek) neve) a BME VIK nyilvánosan hozzáférhető elektronikus formában, a munka teljes szövegét pedig az egyetem belső hálózatán keresztül (vagy autentikált felhasználók számára) közzétegye. Kijelentem, hogy a benyújtott munka és annak elektronikus verziója megegyezik. Dékáni engedéllyel titkosított diplomatervek esetén a dolgozat szövege csak 3 év eltelte után válik hozzáférhetővé.

Budapest, 2017. november 23.

Balogh Tímea
hallgató

Kivonat

Bizonyos informatikai rendszerek üzemeltetése esetén a velük szemben támasztott elsődleges követelmény, hogy ne veszélyeztessenek emberi életeket, ne okozzanak anyagi, természeti károkat. Ilyen úgynevezett biztonságkritikus rendszerek például a vasúti-, repülőgép irányítási berendezések, nukleáris erőművek.

Komplexitásuk miatt ezek tradicionális kód alapú fejlesztését egyre inkább felváltja a modellvezérelt megközelítés, amely során magasszintű modellekből kiindulva, azokat tovább finomítva a rendszer a legapróbb részletekig megtervezhető. A metodika előnyei többek között az automatikus kód-, teszteset- és dokumentáció-generálás, valamint, hogy a létrejövő modellek verifikálásával már a fejlesztés korai szakaszában kiszűrhetők bizonyos hibák.

Ezeken a komplex rendszereken általában egy vagy akár több cég fejlesztő csapatai kollaboratív módon dolgoznak. Így felmerül a modellelemek biztonságának kérdése is, legyen szó olyan bizalmas adatról, létrejövő szellemi tulajdonról, amelyhez csak bizonyos pozíciókban lévő felhasználók férhetnek hozzá, vagy a rendszernek olyan kritikus részéről, amelyet csak megfelelő szaktudással rendelkező fejlesztők módosíthatnak.

A MONDO nemzetközi kutatási projektben készült kollaborációs keretrendszer modellszinten, finomszemcsés szabályok alapján végzi a hozzáférés-vezérlést. Ezekben a szabályokban gráflekérdezésekkel határozható meg, hogy a modellnek milyen típusú vagy pontosan mely elemeire milyen jogok vonatkozzanak különböző felhasználók tekintetében.

Munkám során szöveges szintaxist definiáltam a hozzáférési szabályok meghatározásához, majd implementáltam egy olyan algoritmust, amely képes ilyen szabályok EMF modellek feletti kiértékelésére, vagyis az effektív érvényre jutó hozzáférések kiszámítására. Az algoritmust a már említett MONDO projekt egyik esettanulmányaként használt szélturbina vezérlőről készült modellel teszteltem. Végül az elkészült nyelvtan és algoritmus integrálásra került a kollaborációs keretrendszerbe.

Abstract

1. fejezet

Bevezetés

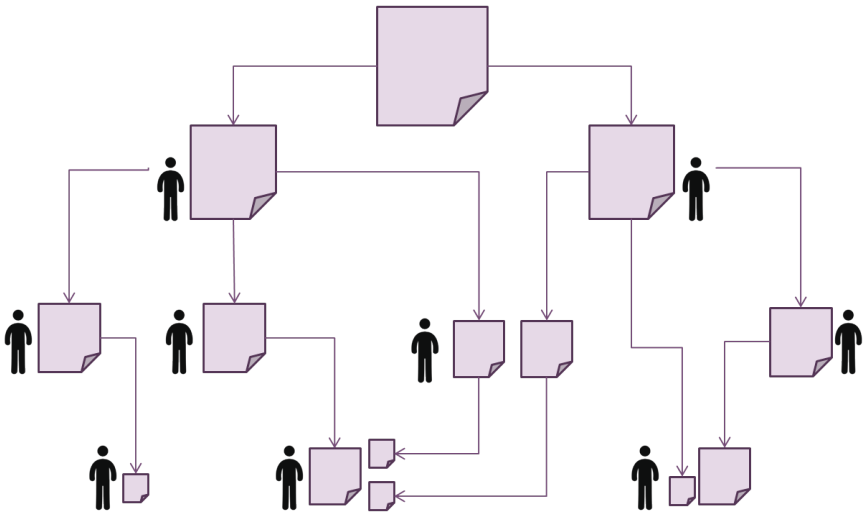
A nagyméretű, komplex ipari szoftverek fejlesztése több ember együttes munkáját igényli. A tervezés modellalapú megközelítése azért is előnyös, mert a magasszintű modellek akár különböző szakterületeken mozgó fejlesztő csapatok számára is ugyanolyan módon értelmezhetők, ami elősegíti a hatékony, összehangolt munkavégzést.

Ezen komplex modellek kollaboratív fejlesztése offline vagy online formában valósul meg. Előbbi esetben a felhasználók egy közös tárhelyen lévő, verziókezelt modellből kérik le a saját példányukat, majd a módosítások végrehajtása után visszaküldik azokat a szerverre. A többiek csak akkor értesülnek ezekről a változásokról, amikor frissítik a sajátjukat a közös modell alapján. Így, ha közben ők is dolgoztak rajta, akkor az összefésülendő verziók között adódhatnak konfliktusok. Ezzel szemben online kollaboráció során a felhasználók által eszközölt változások mindenki számára rögtön láthatók a modellen.

Offline és online forgatókönyv esetén is felmerül a modellelemek biztonságának, hozzáférés-szabályozásnak a kérdése. Abban az esetben például, amikor egy cég a munka egy bizonyos részét ledelegálja egy másik cégnek, az adott modell megfelelő részeit elérhetővé teszi neki. Viszont lehetnek a modellnek bizalmas, a cég szellemi tulajdonának számító elemei, amelyekhez nem akar hozzáférést biztosítani az alvállalkozó számára. Hasonlóan, ha például vannak a modellnek olyan kritikus részei, amelyek fejlesztése speciális szaktudást igényel, akkor ezeket csak a hozzáértő felhasználók módosíthatják, a többiek nem férhetnek hozzájuk.

Modellek feletti hozzáférés-kezelésre létező gyakorlat, hogy a modelleket, modellrészeket tartalmazó fájlokhoz határoznak meg olvasási, írási jogosultságokat. A rendszert újabb felhasználókkal, és számukra meghatározott hozzáférési szabályokkal bővítve a modell megfelelő fragmenseit le kell választani, és külön fájlban eltárolni. Ezt a jelenséget szemlélteti az 1.1 ábra, ennek hatására a modell elemek ezreire aprózódhat. A fájlszintű szabályozás hátránya, hogy ez a jelenség a rendszert nehezen skálázhatóvá, rugalmatlanná teszi.

Erre a problémára a hozzáférések modellszintű szabályozása nyújt megoldást. A MONDO nemzetközi kutatási projektben készült kollaborációs keretrendszer finomszemcsés szabályok alapján végzi a hozzáférés-vezérlést. Ezekben a modell elemi részeire, objektumokra és azok attribútumaira, referenciáira külön-külön lehet hozzáférési jogokat meghatározni a különböző felhasználók tekintetében. A kérdéses modellelemeket gráflekérdezés eredmé-



1.1. ábra. *A fájlszintű hozzáférés-szabályozás problémája*

nyeként kapjuk, amely úgy is megfogalmazható, hogy tetszőleges számú és tulajdonságú elemet adjon vissza. Így egy milliós nagyságrendű modell esetén nem szükséges egyesével minden egyes elemre leírni a jogosultságokat. A finomszemcsézettségből fakadóan a megadott szabályok között előfordulhat konfliktus, inkonzisztencia. Ezek feloldásához szükséges egy olyan kiértékelő komponens, ami eredményként az effektív, valóban érvényre jutó hozzáférési szabályokat adja.

A szakdolgozat kidolgozása során kitűzött célok:

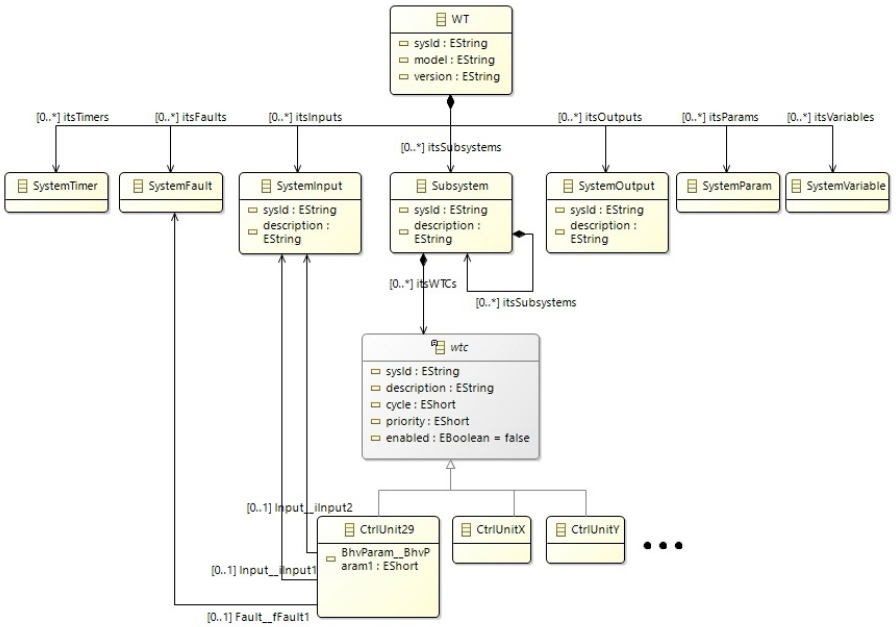
- Szöveges szintaxis definiálása lekérdezés alapú, finomszemcsés szabályok megfogalmazásához
- EMF modellek felett a fenti nyelven megadott szabályok kiértékelését végző algoritmus implementálása, ami
  - megvizsgálva az explicit megadott szabályokat,
  - megtartva a modell belső konzisztenciáját,
  - kiválasztja közülük azokat, amelyek érvényre jutnak
- Az algoritmus működésének bemutatása, teljesítményének kiértékelése egy részletesen kidolgozott esettanulmányon

2. fejezet

Esettanulmány

2.1. Modell

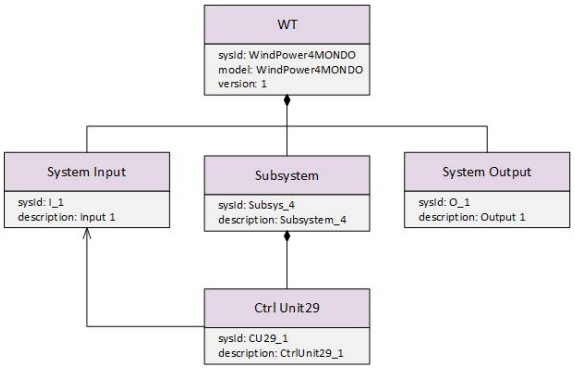
Nagy, összetett ipari rendszerek tervezésében széles körben elterjedt módszer a modellvezérelt szoftverfejlesztés. Az ehhez jelenleg rendelkezésre álló modellezőeszközök gyakran ütköznek skálázhatósági korlátokba. A MONDO EU FP7 kutatási projekt célja ezen kihívások megoldása olyan technológiák, algoritmusok, eszközök kifejlesztésével, amelyek a mostaninál nagyobb hatékonyságot, rugalmasságot biztosítanak a rendszermodellezés terén. A projekt nemzetközi ipari résztvevői közül egy szélturbinavezérlő egységeket összefogó rendszer esettanulmányát vizsgáltam. A rendszer leegyszerűsített struktúráját a 2.1 ábrán lévő Ecore metamodell szemlélteti.



2.1. ábra. *Szélturbinavezérlők metamodellje*

A modell gyökéreleme maga a szélturbina (WT - Wind Turbine), ami további egymásba ágyazható alrendszerekben (Subsystem) tárolja a vezérlőegységek (CtrlUnit - Control Unit)

bővíthető halmazát az őket azonosító, leíró attribútumaikkal, valamint a modell többi elemére hivatkozó referenciáikkal. Ezek az egységek a megegyező attribútumaikat tároló közös ősből származnak le (wtc - Wind Turbine Controller). A gyökérelem az alrendszereken kívül tartalmaz még bemenetet, kimenetet, időzítőt, hibadetektort, paramétert és változót (Input, Output, Timer, Fault, Param, Variable).



2.2. ábra. *Szélturbinavezérlők példánymodellje*

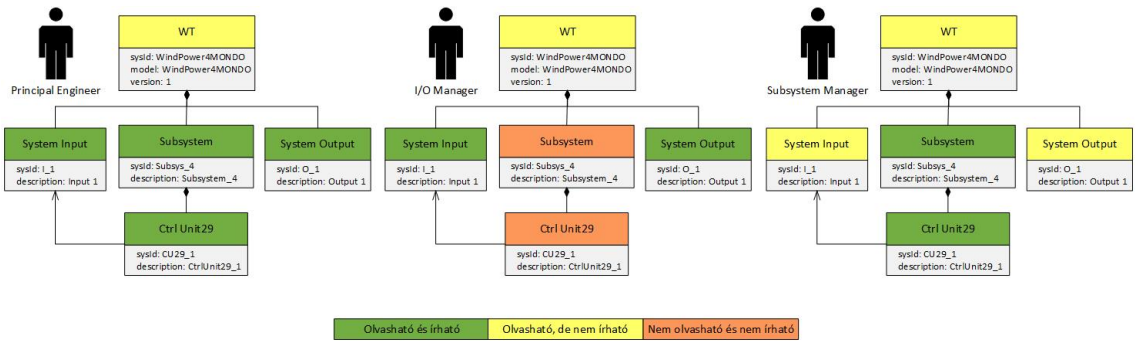
A metamodell egy egyszerű példányát mutatja a 2.2 ábra. A gyökérelem egy vezérlőegységet tartalmaz egy alrendszer alá rendezve, valamint egy-egy bemenetet és kimenetet.

2.2. Feladat

A modell fejlesztése kollaboratív módon zajlik. Ehhez három különböző feladatkörrel rendelkező felhasználótípust definiáltam, akiknek beosztásuk vagy szaktudásuk alapján szükséges meghatározni, hogy a rendszer mely elemei felett rendelkezzenek olvasási és/vagy írási jogokkal. Az érvényesíteni kívánt szabályok a következők:

- A gyökérelemet senki nem módosíthatja.
- Principal Engineer: adminisztrátor jogokkal rendelkezik. A gyökérelemen kívül mindent láthat és módosíthat.
- I/O manager: a be- és kimenetek felelőse, ezeket olvashatja és írhatja, de a modell többi része számára rejtett.
- Subsystem Manager: A Principal Engigeer-hez képest annyival van kevesebb joga, hogy a be- és kimeneteket csak láthatja, de nem módosíthatja.

A feladat ezeknek a szabályoknak egy általam definiált nyelven való megfogalmazása, majd a [cikk]-ben szereplő algoritmus implementálása, ami futásának eredményeképp a modell belső konzisztenciáját megtartva válogatja ki a lenti 2.3 ábrán látható effektív jogosultságokat.



2.3. ábra. *A felhasználók tervezett jogosultságai*

3. fejezet

Háttértechnológiák

4. fejezet

Áttekintés

5. fejezet

Megvalósítás

6. fejezet

Kiértékelés

7. fejezet

Kapcsolódó munkák

8. fejezet

Összefoglalás

Irodalomjegyzék