Intervenciós röntgen berendezés teljesítményszabályozójának automatizált tesztelése

Somogyi Ferenc Attila

2016. December 07.

Szoftver verifikáció és validáció kiselőadás

BME AUT
Automatizálási és
Alkalmazott
Informatikai Tanszék

Forrás

- Mathijs Schuts and Jozef Hooman: **Industrial Application of Domain Specific Languages Combined with Formal Technique,** in Proceedings of the 1st International Workshop on Real World Domain Specific Languages, ACM, 2016.

Miről lesz szó?

- Éles projekt (Philips)
  - Műtéti beavatkozások segítése
    - Intervenciós röntgen berendezés
      - Röntgen képek műtét közben
- Cél: fejlesztés hatékonyságának növelése
  - Szakterületi nyelvek és formális módszerek együttes használata
- Formális módszerek
  - Modell ellenőrzés
  - Automatizált tesztelés
  - Generátorok és modellek validációja

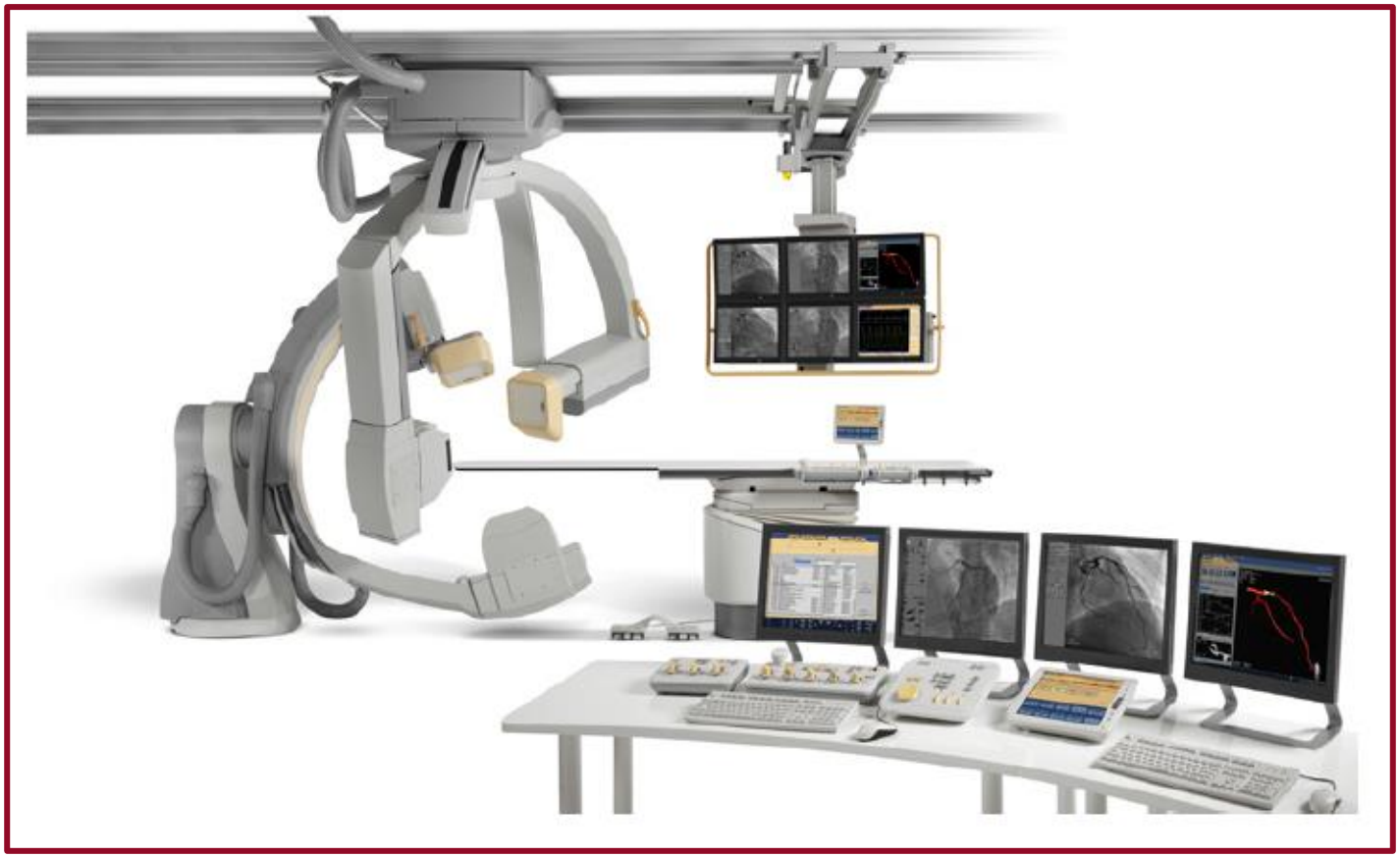
Bevezetés

- Teljesítményszabályozó egység
  - Komponensek indítása, leállítása
  - Alacsony- és magasfeszültségű terminálok
  - Konfiguráció
    - Új release
    - Új hardware konfiguráció
    - Nehezen áttekinthető és módosítható
  - Cél: karbantarthatóság és kiterjeszthetőség
    - Megoldás: DSL bevezetése a konfiguráció megadására (a továbbiakban **konfigurációs DSL**)

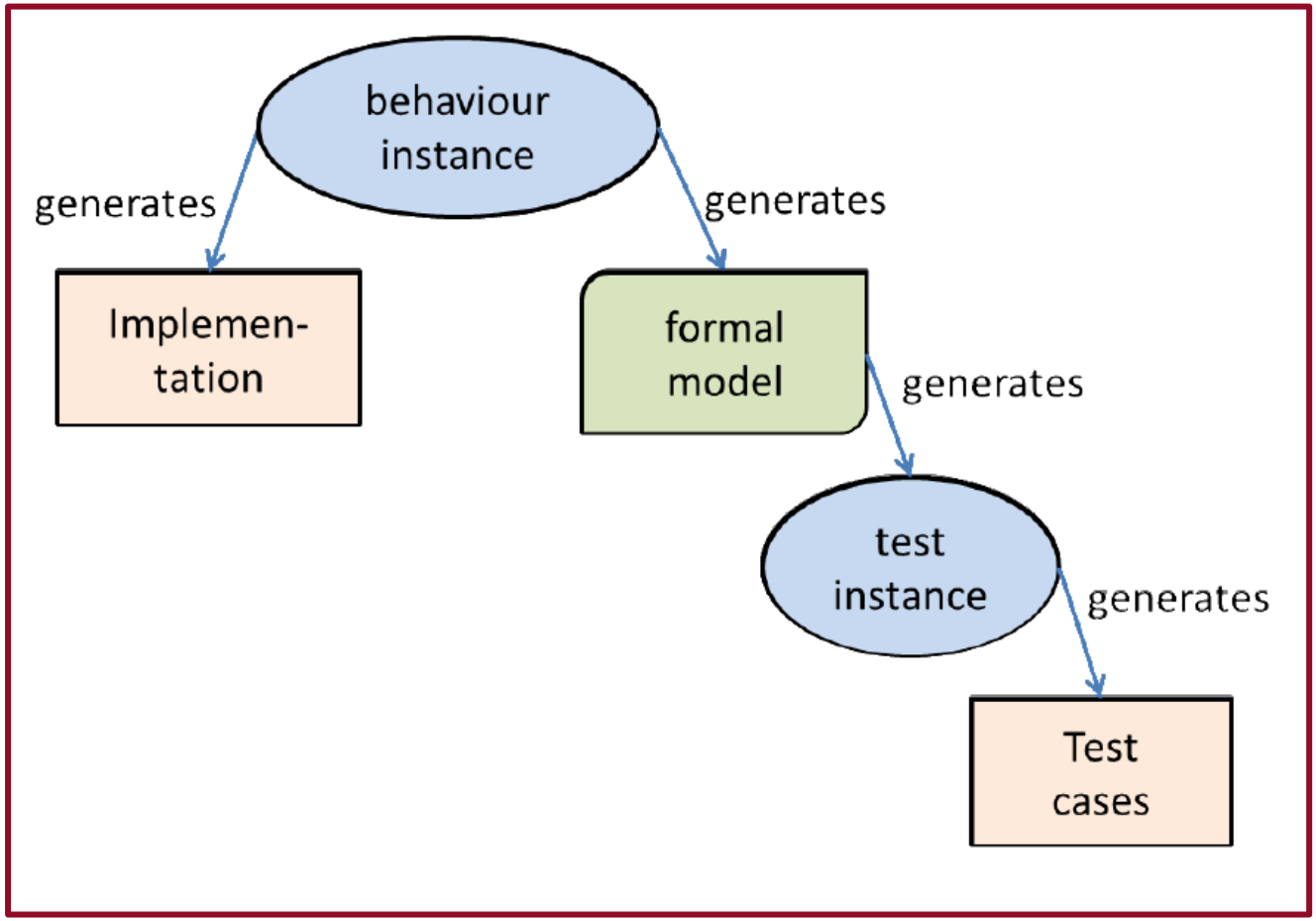
Bevezetés

- Szakterületi nyelvek (**domain-specific languages - DSL**)
  - Szakterületi absztrakció + megjelenítés
  - Nagyobb kifejezőerő, „kényelmesebb” használat
  - Pl. HTML, SQL, Unix Shell Scripts, stb.
- Általános célú nyelvek (**general-purpose languages - GPL**)
  - Általános absztrakció + megjelenítés
  - Általános, több szakterületnél is használható
  - Pl. C, C++, Java, Python, stb.

Bevezetés



A projekt áttekintése



A projekt áttekintése

- Konfigurációs DSL
  - Implementáció és formális modellek generálása
  - Konfigurációs DSL validálása
- Konfiguráció tesztelése
  - **Tesztelési DSL** bevezetése, generálása
- Konfigurációs DSL = „forráskód”
  - Minden ebből generálódik (közvetve)
  - A helyessége nagyon fontos!

Felhasznált technológiák

- **Xtext**
  - DSL-ek definiálása

- **POOSL**
  - Parallel Object-oriented Specification Language
  - Szimuláció (viselkedés)
  - Eclipse támogatás
- **SAL**
  - Symbolic Analysis Laboratory
  - Formális verifikáció
  - Teszt generálás

Konfiguráció

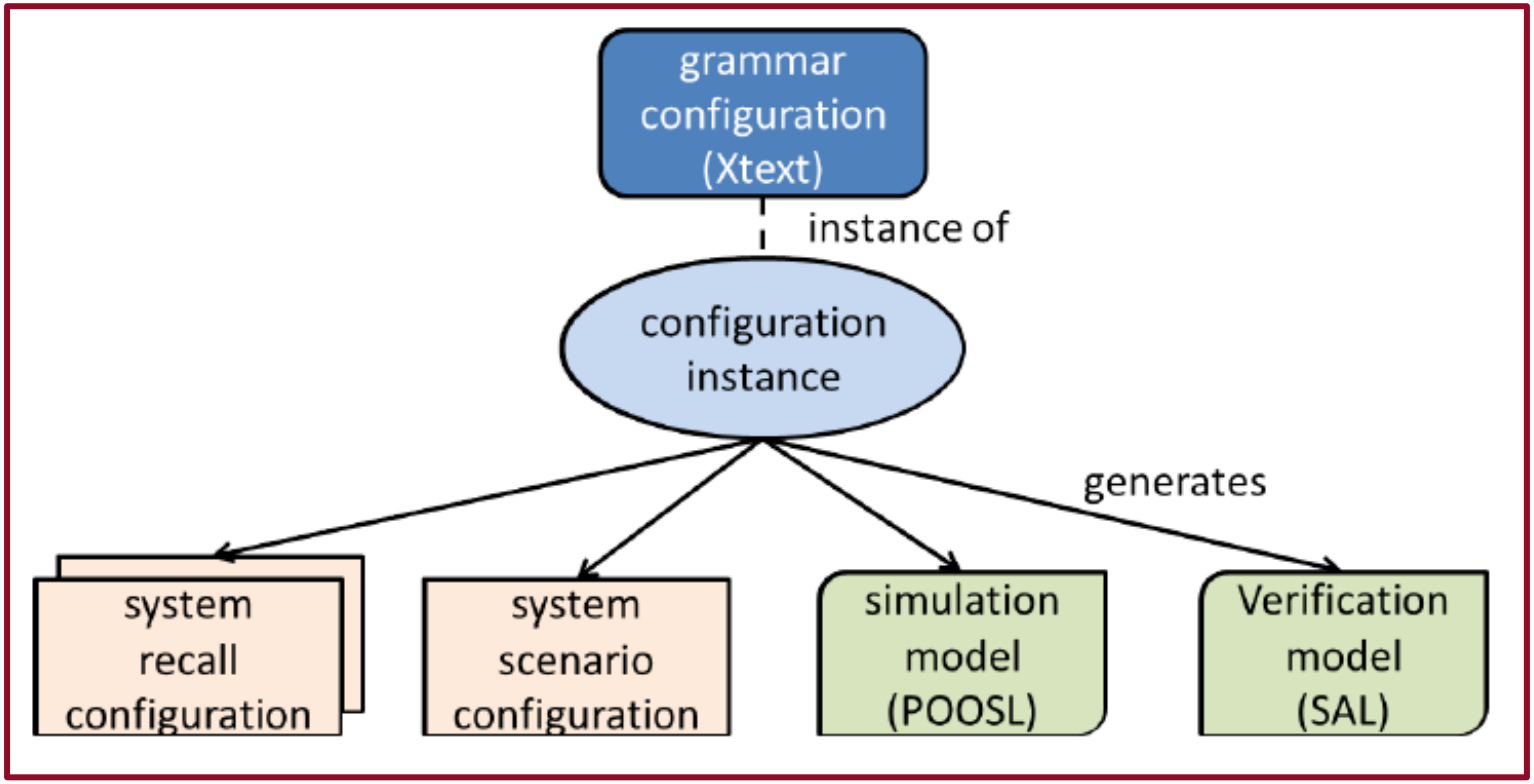
- A röntgen berendezés egy elosztott rendszer
  - Sok hardver és szoftver komponens
  - Magas konfigurálhatóság
    - Röntgen állvány, betegasztal, monitorok, stb.
  - Teljesítményszabályozó + támogató hardware külön szobában
- Teljesítményszabályozó konfigurációja
  - Recalls configuration file
    - Több recall-t tartalmaz
    - Recall = terminális komponensek állapota
  - Scenarios configuration file
    - Forgatókönyv leírása állapotgép segítségével
    - Recall-ok = csomópontok, tranzíciók nem atomiak

Konfiguráció

```
# TermStandby
<RECALL 1>
<TAP>
00 7 1 0.0 0.0 0.0 # Controller_PowerBus, status = On
00 8 0 0.0 0.0 0.0 # Controller_PulsePowerBus, status = Off
04 0 1 0.0 0.0 16.0 # M_Cab_HVT1, status = On
04 1 0 0.0 0.0 16.0 # M_Cab_HVT2, status = Off
...
04 1 1 1 # M_Cab_LVT5V1, status = Off
04 2 1 1 # M_Cab_LVT12V1, status = Off
04 5 1 0 # M_Cab_LVTGbl, status = On
```

```
2 2 0 00000000 00000000 112 4 2     # recall 2 exit out of forced off
```

A konfigurációs DSL



A konfigurációs DSL

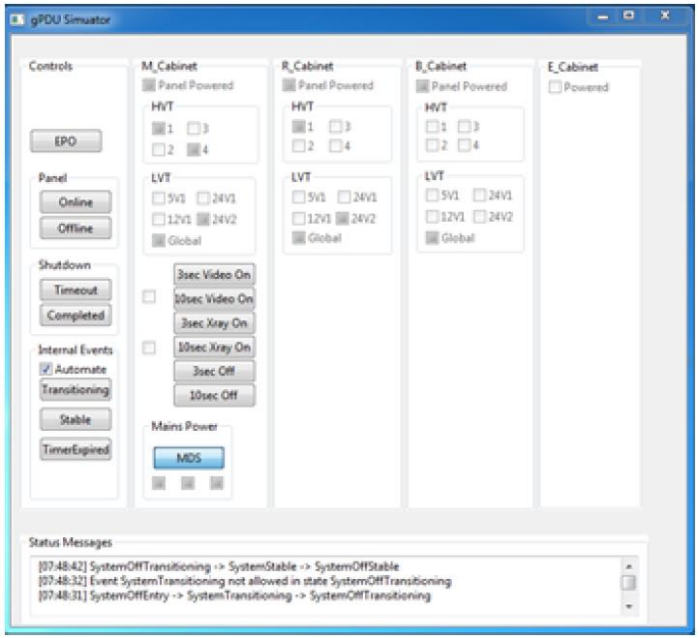
```
termstatuses = SystemInit or SystemOff or
               SystemFseOff or SystemOn …
…
group = SystemFseOff and SystemEPO    recallID = AllOff
group = SystemOff and SystemOffError recall = TermStandby
group = SystemOn and SystemOnError    recallID = AllOn
…
state Init
    termstatus SystemInit
         if Transitioning stim PostFail
                              next termstatus SystemStop
                         stim Initialized
                              next termstatus SystemOff
state Standby
    termstatus SystemFseOff
                         stim EpoActive
                               next termstatus SystemEPO
         if Stable       stim ButtonOn3sec
                              next termstatus SystemOn
    termstatus SystemOff
         if Stable       stim ButtonOn3sec
                              next termstatus SystemToggleTaps
                         stim ButtonOff10sec
                              next termstatus SystemFseOff
                         stim EpoActive
                              next termstatus SystemEPO
    termstatus ShuttingDownSystem
         if Transitioning stim ShutdownTimedOut
                              next termstatus SystemOff
                         stim ShutdownCompleted
                              next termstatus SystemOff
                         stim EpoActive
                              next termstatus SystemEPO
…
```

```
...
config name = setup
    recall TermStandby
        Default for recall        status Off
            Controller
                PowerBus          status On
            M_Cab
                HVT1              status On
                HVT4              status On
                LVT24V2a3         status On
                LVTGbl            status On
...

config name = setup_derived1
    recall TermStandby
        Use config setup
            M_Cab
                LVT24V2a3         status Off
    recall TermToggle
        Use config setup
    recall TermShutDown
        Use config setup
```

Szimuláció

- POOSL modell generálása
  - > Konfigurációs DSL-ből
  - > GUI-hoz kapcsolódik socket-ek segítségével
- Szimuláció célja
  - > Viselkedés (konfiguráció) validálása



Formális verifikáció

- SAL
  - Modellellenőrzés, tesztgenerálás, stb.
  - Formális modell generálása konfigurációs DSL-ből
- Modellellenőrzés
  - Linear Temporal Logic (**LTL**)
  - Invariánsok teljesülése a modellen
  - Konfigurációs fájl generálás csak ezután!

Formális verifikáció

```
SALModel: CONTEXT =
BEGIN
 State : TYPE = {SystemOnStable, SystemPartlyOnStable, ...};
 Stim : TYPE = {ButtonOn3sec, ButtonOn10sec, ButtonOff, ...};
main : MODULE =
 BEGIN
 INPUT stim : Stim
 OUTPUT state : State
 LOCAL Controller_PowerBus, M_Cab_HVT1, ... : BOOLEAN
 INITIALIZATION state = SystemOffStable;
                Controller_PowerBus = TRUE;
                Controller_PulsePowerBus = FALSE; ...
 TRANSITION
 [ state = SystemOffStable AND stim = ButtonOn3sec
    −− > state' = SystemToggleTapsStable;
                Controller_PowerBus' = TRUE;
                Controller_PulsePowerBus' = TRUE; ...
 [] state = SystemOffStable AND stim = ButtonPartlyOn3sec
    −− > state' = SystemPartlyOnStable;
                Controller_PowerBus' = TRUE;
                Controller_PulsePowerBus' = FALSE; ...
 [] ELSE −− > %  implicitly: state'= state
 ]
 END;
% Properties
END
```

```
th1: THEOREM main |−
G(Controller_PowerBus = M_Cab_HVT1 = M_Cab_HVT2 =
          R_Cab_HVT4 = B_Cab_HVT3) AND
...
G(M_Cab_HVT1 = M_Cab_HVT2);

th2: THEOREM main |−
G((state = SystemOffStable AND M_Cab_HVT4) =>
        G(state = SystemPartlyOnStable => M_Cab_HVT4))
AND
G((state = SystemPartlyOnStable AND M_Cab_HVT4) =>
        G(state = SystemOnStable => M_Cab_HVT4))
AND
...

th3: THEOREM main |−
FORALL (i: State): ((NOT(i = SystemToggleTapsStable)) =>
        M_Cab_LVT24V2a3);

th4: THEOREM main |−
G(M_Cab_LVT5V1 => M_Cab_LVTGbl) AND
G(M_Cab_LVTGbl => M_Cab_HVT1) AND
...
G(R_Cab_LVT5V1 => R_Cab_LVTGbl) AND
G(R_Cab_LVTGbl => R_Cab_HVT1) AND
```

Tesztelés

- Előre definiált tesztesetek
- Dedikált teszt tool
  - > CSV fájl
  - > Oszlopok: parancs, válasz, idő / event, komment
  - > Teszt végrehajtása, riport készítése

PDS:SYST?	6:00:00	2500	SystemEPOEntry
PDS:QUE109:PAR-1	No Error	2500	ButtonOn10sec
PDS:FWV?	3.0.0.0	T016_TRANS	SystemTransitioning
PDS:SYST?	3:01:02	1000	SystemOnTransitioning
PDS:FWV?	3.0.0.0	T017_STABLE	SystemStable
PDS:SYST?	3:02:02	1000	SystemOnStable

Tesztelési DSL

- Egyszerűbb leírás
  - Traceset, trace-ek – teszteset generálás
- Automatikus teszteset generálás
  - SAL modell alapján (kiegészítve)
  - Tesztelési DSL példány generálása (trace-ek)

Tesztelési DSL + SAL modell

```
termstatuses
termstatus SystemFseOffEntry code "2:0:0"
termstatus SystemFseOffTransitioning code "2:1:0"
termstatus SystemFseOffStable code "2:2:0"
–
transitions
transition EpoActive from termstatus SystemFseOffEntry
                      to termstatus SystemEPOEntry
transition EpoActive from termstatus SystemFseOffTransitioning
                       to termstatus SystemEPOEntry
transition ButtonOn3sec from termstatus SystemFseOffStable
                         to termstatus SystemOnEntry
–
tracesets
traceset SystemEPOEntry
trace SystemEPOEntry -> ButtonOn10sec -> SystemOnEntry ->
SystemTransitioning -> SystemOnTransitioning -> SystemStable ->
–
SystemEPOEntry
–
```

```
...
LOCAL t0, t1, t2, t3, t4, ...,
INITIALIZATION state = SystemOffStable;
                t0 = t1 = ... = FALSE  ...
TRANSITION
[ state = SystemOffStable AND stim = ButtonOn3sec
      −− > state' = SystemToggleTapsStable;
                t0' = TRUE; Controller_PowerBus' = TRUE; ...
[] state = SystemOffStable AND stim = ButtonVideoOn3sec
      −− > state' = SystemVideoOnStable;
                t1' = TRUE; Controller_PowerBus' = TRUE; ...
[] ELSE −− >
]
END;
% Properties
END
```

Modellek és generátorok validációja

- Log fájlok
  - Tesztelőktől és valós felhasználóktól
  - Trace transzformálás (tesztelési DSL formátuma)
- POOSL modell validálása
  - Másik POOSL processz (GUI helyett input)
  - Teszt trace használata (stimuli, output)
- SAL modell validálása
  - LTL formula: teszt trace

```
th11: THEOREM main |–
G((state = SystemOffStable AND stim = ButtonPartlyOn3sec) =>
   X(state = SystemPartlyOnStable)) AND
G((state = SystemPartlyOnStable AND stim = ButtonOff) =>
   X(state = ShuttingDownPartlySystemTransitioning)) AND
G((state = ShuttingDownPartlySystemTransitioning AND
       stim = ShutdownCompleted) =>
   X(state = SystemOffStable));
```

Konklúzió

- Karbantarthatóság és kiterjeszthetőség
- Szakterületi nyelvek + formális módszerek = hatékonyság
- Statisztika
  - > DSL-ek elkészítése: ~35 óra
  - > POOSL és SAL generátorok: ~ 5-5 óra
  - > Új release: közel kétszer akkora konfigurációs fájlok
    - A bemutatott megoldással kezelhető
    - ~60 óra helyett ~8 óra!
- Más, hasonló projektekben is bevezették a módszert

Köszönöm a figyelmet!