VARiability In safety-critical Embedded Systems

ARTEMIS-2011-1
Project Number: 295397

BVR – Better Variability Results

by Øystein Haugen (SINTEF) and Ommund Øgård (Autronica)
What do we mean by “variability”?

- **Product Line variance**
  - often variants of the same software base
- **Cross-cutting variability**
  - often variability is orthogonal to the software design
  - variability needs are discovered after the first software design
- **The variability designer is not always the software designer**
  - division of labor and of competences
The Autronica Product Family

- **AutroMaster**
  Top level graphical presentation system running on Linux PCs

- **FireAlarmSystem**
  System consisting of embedded fire panels with logics and LCD menu system.

- **AutroSafe**
  High end networked Fire Alarm System for large demanding applications

- **Autroprime**
  Medium range standalone Fire Alarm System

- **FieldEquipment**
  Smoke detectors, manual call points, sounders, IO units etc.
The Market Domains of Autronica

Autronica – turnover 2010

- Turnover 2010: NOK 760 mill

- The maritime market: 27.6%
- The petrochemical, oil & gas market: 33.6%
- Onshore market – Norway: 28.8%
- The international onshore market: 10.1%
**Common Variability Language (CVL)**

- **Generic & Standardized**
  - CVL

- **Focused on a domain**
  - DSL

- **Specification in CVL of base model variabilities**
  - Variability model

- **Base model**

- **Execute CVL**
  - Resolution models
  - Selection of a set of choices in the variation model
  - Resolved models

- **Product line model in any MOF-compliant language**

- **Product models fully described in the base language**
  - All regular base language tools can be applied to these models
CVL Architecture

Base Model

Variability Realization

Configurable Units

Variability Interfaces

Variation Points

VSpecs

Constraints

Variability Abstraction

Resolutions
The MOF2CVL experiment
Introducing a simple car configuration

Duplicating choices – not legal CVL

Unique choices, supplemented by constraints
Constraints are about targets

- "Parkassist implies hp140" means that either (Manual, AWD, hp140) or (Automatic, AWD, hp140) are valid
- Constraints are about "targets" and not about decisions
- Duplicated names on VSpecs indicate that they are decisions on the same target
Autronica Variability model (Type/Inst.)
Introducing VSpec Type

Note that hp140 refers to any hp140 instance

indicating scope/ownership

type AWD definition

instance of type AWD

 config

configurable unit

Yeti

Laurin & Klement

type AWD

instance of type AWD

Parkassist implies hp140

Manual

FWD

awdmanual: AWD

Automatic

hp140

hp110

awdaumatic: AWD

hp110
Cascading effects of VSpec Type

- Configurable Units
- Variability Interfaces
- Variation Points
- Variability Realization
- VSpecs
- Constraints
- Resolutions
- Staged Variation Point
- VSpec type
- Targets
- Base Model
- Literals
Realization (additive, nested)
Realization (subtractive)

Problem is that these fragment substitutions do not know the resolution of the Engine!

This one does not know which wheel!
Realization (staged realization)

Here all the information of resolution is available.
Resolution Literals

 literal
 Strong:Engine

 literal
 Weak:Engine

 w1:Engine=Strong
 w2:Engine=Strong
 w3:Engine=Weak
 w4:Engine=Weak

 kW500 = true
 kW300 = true

 w1.Engine=Strong w2.Engine=Strong w3.Engine=Weak w4.Engine=Weak

 kw300 kw500 kw300 kw500

 Staged
 VariationPoint

 Staged
 VariationPoint

 Fragment
 Substitution

 Fragment
 Substitution

 Fragment
 Substitution

 Fragment
 Substitution
New in BVR

- Configurable Units
- Variability Interfaces
- Variation Points
- Variability Realization
- VSpecs
- Constraints
- Resolutions
- Variability Abstraction
- Note
- Reference
- VSpec type
- Targets
- Staged Variation Point
- Base Model
- Literals